IRON MOUNTAIN®

WHITE PAPER

DataDefense™

PROTECTING SENSITIVE CORPORATE DATA

Mobile devices improve productivity, but increase the risk of compromising sensitive data

Consider the data that resides on your organization's laptops. Do those laptops contain client information, intellectual property, customer identity files, financial plans or other sensitive and valuable data? What would happen if that data were to end up in the wrong hands? The answer is all too evident.

A single data loss event can cost a company millions of dollars. Negative publicity, loss of brand reputation, costly litigation, and reduced competitive advantage are among the possible consequences. In addition, much of the data resident on computers is subject to provisions of various federal and state laws, some of which carry significant financial penalties.

Today, most data is protected with sign-on passwords at the operating system level. Because many people use simple passwords that are easy to remember, it also makes them easier to crack. Significant effort is being made to encourage the use of stronger passwords. Unfortunately, users may feel compelled to write down more complex passwords to prevent forgetting them, negating their benefit.

Companies that use tokens or other external authentication devices depend on users keeping the tokens secure and separate from their laptop computer. Naturally, users prefer to carry the token with the computer to ensure that they don't misplace it, thereby undermining the security of a token system in the first place.

Encryption alone, while important, still depends on the above access controls. Additionally, use of whole disk encryption may add significant inconvenience to both the users and the administrators of the devices. For example, secondary encryption passwords are often used which adds to user and Help Desk support burdens, it may add enough CPU cycle overhead to be annoying to users, and it may interfere with operating system security and disk utilities.

Destruction of sensitive data is the best way to secure it

When faced with the scenario of a stolen laptop, most business leaders would choose to destroy the data on the device rather than just conceal it. Destroying the data insures that no one will have access to it, no matter what methods they employ.

Some of the laws governing data security:

- Sarbanes-Oxley
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (HIPAA)
- California Security Breach Information Act (SB 1386)
- Federal Information Security Management Act (FISMA)
- Fair and Accurate Credit Transactions Act (FACTA)

Mobile data is particularly at risk:

- Data breaches shaved about 1% off the stocks (of affected companies) right away, causing them to under perform the broader market, and there's some indication of a more serious, long-term effect. *(Source: Wall Street Journal June 15, 2005)*
- About 10% of all laptops will be stolen, and less than 3% of these are likely to be recovered. *(Source: IT Architect 2005)*
- Laptop theft is the second most prevalent form of computer attack, behind only viruses. *(Source: 2005 CSI/FBI Survey)*
- As much as 60% of corporate data resides unprotected on PC desktops and laptops. *(Source: IDC Analyst)*

DOCUMENT INFORMATION
Protecting Sensitive Corporate Data

PRINTED
February 2006

COPYRIGHT

TRADEMARKS

DISCLAIMER
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. The information in this document is subject to change without notice and should not be considered a commitment by Iron Mountain.

TABLE OF CONTENTS

ABOUT IRON MOUNTAIN INCORPORATED

Iron Mountain Incorporated (NYSE:IRM) is the world's trusted partner for records management and data protection services. Founded in 1951, the Company has grown to service more than 235,000 customer accounts throughout the United States, Canada, Europe and Latin America and the Pacific Rim. Iron Mountain offers records management services for both physical and digital media, disaster recovery support services, and consulting — services that help businesses save money and manage risks associated with legal and regulatory compliance, protection of vital assets, and business continuity challenges. The DataDefense™ application is a complete encryption and security solution that is both simple to administer and user transparent, and will automatically eliminate data on lost or stolen computers.

For more information visit www.ironmountain.com

INTRODUCING DATADEFENSE

Until now, business leaders have been forced to depend on end user compliance with corporate security policies to protect sensitive data. The DataDefense solution by Iron Mountain removes the need for special end user compliance and returns control and safeguarding of data to business leaders and IT management.

DataDefense is Efficient and Easy to Administer

The DataDefense solution is centrally administered through a web-enabled interface, giving business owners control over their data with a variety of device settings and event-driven rules that can trigger actions to enforce organizational security policies. The DataDefense settings and rules can be used individually, or in combination, to enable you to tailor the DataDefense controls to meet your organization's specific needs. Because it is centrally administered, DataDefense ensures business owner control of sensitive data without additional reliance on the policy compliance of individual end users.

DataDefense is Transparent so End User Acceptance is Assured

Business leaders have long been forced to depend on PC users' compliance with organizational security policies to protect sensitive corporate data. Unfortunately, users concerned with immediate business needs and personal productivity often sidestep these policies because they can be burdensome. The DataDefense solution provides silent mobile policy enforcement which removes compliance obligations from the user. DataDefense is completely transparent to the user, therefore, there is no training required or new passwords to remember. In fact users will not need to alter their usual behavior at all.

Multi-Layered Approach Ensures Administrator Control Over Many Threats

DataDefense, a solution engineered to provide a PC data security tool that anticipates a multitude of threats, operational scenarios and user behaviors. The DataDefense application can detect behaviors which are inconsistent with authorized use and swiftly take action to eliminate the possibility of a security breach. Administrators can also use the DataDefense application to proactively enforce security policy. For example, a date and time can be chosen to eliminate specific files from any group of devices. In addition, the DataDefense solution will take pre-set administrator prescribed actions even when the device is removed from the network and internet.

Using its proprietary custom interface, the DataDefense solution also allows the business owner to centrally deploy and intelligently manage the Microsoft® Windows® Encrypting File System (EFS), which may be used in place of other costly and burdensome encryption products.

How DataDefense Works

If, for example, an employee loses a laptop containing company data and a thief attempts to crack the logon password, the DataDefense solution would recognize the attack and trigger one or more "Failed Logon Attempt" rules, either concurrently or in succession, which would take action like destroying the sensitive data.

In another situation, a manager reports that her laptop has been stolen. The DataDefense administrator changes her computer's DataDefense status to "Stolen." The next time the computer checks in via the internet, it receives a destruct command and the sensitive data on the hard drive is immediately destroyed.

If the thief fails to connect the device to the internet, thereby preventing the device from checking in with the DataDefense Server, special timers will expire and the data is destroyed anyway. Data may be overwritten then deleted; customized warnings and persistent system shutdowns are available as well.

ENHANCING AND EXTENDING SECURITY

Security of electronic data can be viewed in layers. There are some basic layers such as physical security and logon passwords that most companies routinely employ to secure data. This is similar to locking your front door and arming the alarm system when you leave home. The shortfall is that once a thief has breached these basic measures, they have full access to the device, the data residing on it, and can use it to gain access to corporate resources.

The typical security model is enhanced by integrating DataDefense with your traditional layers of security. The addition of the DataDefense solution to your security suite allows you to extend security into the domain where the user has full access while still providing data security even as the user is using the device.

Encryption is also used and extended beyond the typical security model into the area where the user has full access. This allows the administrator to continue to apply additional encryption beyond what the typical user might employ.

The way the DataDefense solution secures data is to eliminate it from a compromised device when it detects a threat. Threats that are monitored are removal of the device from the network, and failed logon attempts. The DataDefense solution can be customized, thereby allowing you the ability to provide the most optimum data security for your company's devices. The following sections discuss how the DataDefense solution monitors and secures your data.

Encryption

Encryption is the process of converting data into a format that cannot be read by others. Enabling encryption in the DataDefense service turns on the Microsoft Encrypting File System (EFS) built into the Microsoft Windows 2000 and Windows XP Professional operating systems. The DataDefense solution enables you to centrally and intelligently define and automatically encrypt all data files in any location on any local drive of each device. You can specify the location(s) of your important files using standard Microsoft Windows locations, such as My Documents, by using traditional file system paths to target non-standard folders, or by specifying files of a particular type (e.g., all .doc files).

Encrypting files prevents unauthorized users from directly accessing files on your hard disk drive. For example, if your computer had been stolen and the thief was unable to login, he might then attempt to boot from a CD or even remove the hard disk drive and connect it to another computer in order to access the data. In this scenario, the thief might be able to access the files, but would be unable to decrypt them, thereby making the files unusable.

Under normal circumstances, when a user opens an encrypted file it is automatically decrypted by the Microsoft Encrypting File System. The encryption and decryption activities happen in the background and are transparent to the user. Encryption is controlled with encryption keys that are directly tied to the user's login. When a user successfully logs in, the encryption keys are unlocked and encrypted files are accessible to him. To thoroughly secure encrypted files, it is important to create rules for your devices that will delete the encryption keys (EFS Certificates) for the user's account in the event that the device is compromised. This is the quickest method for making data inaccessible. And, if you have a backup of the EFS Certificates, it is also the quickest way to recover your data should you be fortunate enough to eventually recover the device.

Failed Login Attempts

One of the events monitored by the DataDefense service is the number of sequential failed login attempts that occur across all accounts on a device. By creating a rule that allows only a few failed login attempts (incorrect username and/or password) you prevent an unauthorized user from having an unlimited amount of time to guess the login information. As soon as the number of failed login attempts is reached (the threshold), the computer will either display a message, shut down, or start destroying files as you have specified in the rule settings. You can set the number of failed attempts to any number between 3 and 15. It is important to select a threshold that is appropriately tight so you do not provide a thief additional time to attempt to access data on the device.

You can create multiple layers of rules that monitor invalid login attempts where the severity of the action escalates as additional failed attempts are detected (e.g., after three failed login attempts, a message is displayed, after six, the EFS Certificates are deleted, after nine attempts, additional files are deleted). The number of invalid login attempts continues to accumulate until a valid login occurs. At that point, the invalid login counter is reset to zero.

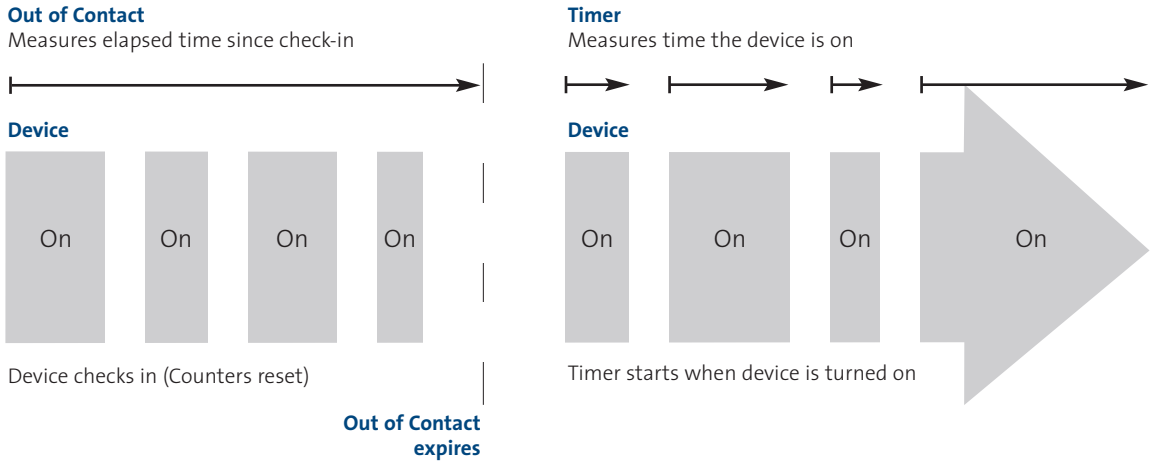
In order to achieve a greater level of security for your data, it is important that users choose a password that is difficult to guess. If they use the name of a spouse, child, or pet, it may be easy for a thief to guess the password in only a few attempts. The use of strong passwords that require a combination of letters, numbers, and symbols, is highly recommended.

Out of Contact

In the event that someone is successful at guessing the login username and password or the device has been absent for an extended period of time, the Out of Contact time period provides an additional measure of security. The DataDefense service requires each device to check in with the DataDefense Server via a network connection on a regular basis. If the period of time between check-ins is exceeded (Out of Contact), an action is triggered. In other words, if an unauthorized person removes network access from a device and has managed to gain access to your computer by successfully logging on, he still only has a small window of time to access data on the device before sensitive data is destroyed because the device has been out of contact for too long.

Out of Contact rules and actions are based on the period of time elapsing between certain computer and operating system events. There are standard check-in events that occur at startup, shutdown, login, logoff, lock, unlock, and when a new network connection is made, where the device automatically establishes a connection and checks in with the DataDefense™ Server. There are also periodic check-ins that happen while the device is online. At regular intervals, the DataDefense Agent automatically establishes a connection with the DataDefense Server and checks for any rule or status changes since the last time it checked in.

The Out of Contact time period allows a device to be offline (and not checking in) for a specified period of time (overnight, or over a weekend). There is a second component to the Out of Contact time period, known as the Timer. It allows an additional amount of time after the Out of Contact time period has expired before actions are triggered (a grace period). The important difference between the two is that the Out of Contact time period is linear (total elapsed time from the last check-in) and the Timer is cumulative uptime (the amount of time the device is switched on).



Relationship Between Out of Contact and Timer

An optional warning message can be used to warn the user that the Timer has been activated. You can customize the message so that it makes sense to the owner of the device, but would be less alerting to a would-be thief. For example, the message can instruct the employee to call the Help Desk and report an error code. The error code indicates to the support person that the Timer on the device is now active.

To understand how Out of Contact functions to protect sensitive data from being compromised, consider the following example. By default, the Out of Contact time period is set to 2 weeks and the Timer is set to 12 hours. In addition, a warning message will be displayed twice while the Timer is active. Let's assume the employee goes on vacation for 1 week but decides to extend his/her vacation for an additional week. It's possible that the Out of Contact period will expire depending upon when the device last checked in with the DataDefense Server. Let's assume it has expired. If the device remains off until the employee returns from vacation, then only the Out of Contact time period will have expired and the Timer will not have been initiated since the device is off. Once the device is turned on, the Timer will start. In addition, a warning message will be displayed at the onset of the Timer and a second one will appear once half of the Timer period has been used. Once the device is booted, the DataDefense Agent will attempt to check in, repeat the attempt when the employee logs into the computer, and again once the employee establishes a network connection to check email. Upon a successful check-in with the DataDefense Server, all the time periods are reset. Otherwise, Out of Contact continues to measure elapsed time.

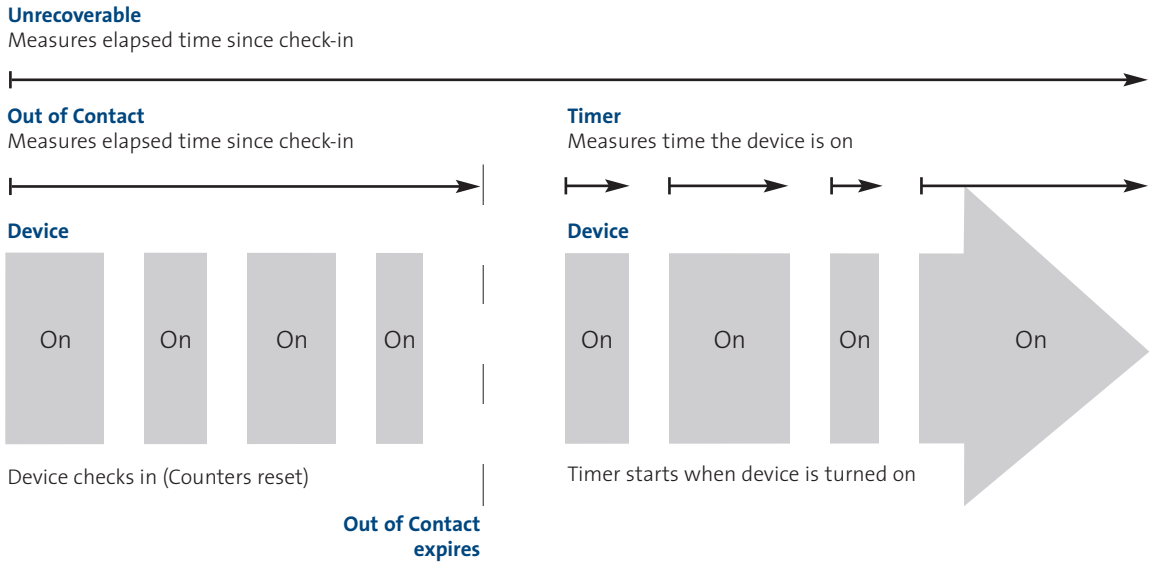
To understand how the Timer measures time, a 12 hour Timer means the employee can use the device for 12 continuous hours or 1-1/2 8-hour work days, assuming the device is powered on during the workday. However, since the Timer only measures the time the computer is powered on, a 12 hour Timer could be stretched out for several days, if not weeks, depending upon how often and for what duration the computer is used.

Device Status and Unrecoverable

If a device is ever lost or stolen, there are two methods that are used to initiate data security actions. First, the administrator can proactively change the status of a device as soon as it is reported lost or stolen, and direct the DataDefense Agent to immediately destroy data on the device. The next time the device checks in with the DataDefense Server, such as at system boot, it will see that its status has been changed to Stolen, and immediately execute all "Device is Stolen" rules. These actions are taken even if the Invalid Login rules or Out of Contact rules have not yet been triggered.

If a lost or stolen device never checks in with the DataDefense Server, the device status cannot be communicated to it. In this case, the final measure is the Unrecoverable time period. This timer is similar to Out of Contact in that it is a measure of total elapsed time, however, unlike Out of Contact, the Unrecoverable time period does not have a Timer component. The time periods associated with Unrecoverable are in months, as the assumption is that if a device has not contacted the DataDefense Server for an extended period of time, it is truly unrecoverable and will never be returned.

When the device is booted, the DataDefense Agent will attempt to check-in with the DataDefense Server. If successful, the timers are reset; however, if unsuccessful and the Unrecoverable timer has expired, the rules associated with Unrecoverable will execute immediately. When considering Out of Contact and Unrecoverable, both measure time, however, since Out of Contact also has the Timer, which acts as a grace period, it is a race condition to see which time component expires first.



Relationship Between Out of Contact and Unrecoverable

Date and Time

The DataDefense service includes an additional layer of security that initiates an action at a pre-determined future date and time. Known as Date & Time, these rules are triggered at the time you set, if the device is powered on, whether or not it is connected to the internet. If the device is off when the date and time occurs, the action will be triggered immediately when the device is powered on. The time granularity available is in one hour increments. Available actions range from the non-destructive actions of displaying a message or logging the event, to the destructive actions of Secure delete files or DOD delete files.

Date & Time rules are extremely useful for deleting retired data from devices for compliance purposes or to ensure employees are no longer using documents containing time-sensitive data.

RESTRICTING ACCESS TO DATA

There are several actions that the DataDefense service can perform to restrict access to your data when unauthorized events are detected. These actions can be divided into two groups, non-destructive and destructive.

Non-destructive actions

- Display message – Allows the DataDefense administrator to display a pre-defined message on the device when an event threshold is reached. This is a non-destructive action and does nothing more than simply display a message to the user.
- Log event – Logs the event and sends it to the DataDefense server where it can be viewed by the DataDefense administrator. If the device is not connected to a network, the event is placed in a queue and sent during the next successful server check-in. This is also a non-destructive event and does nothing more than alert the DataDefense administrator that certain event thresholds have been exceeded.
- Shutdown – The device powers off after the predetermined number of failed logons or upon the expiration of a pre-defined date and time. Turning the device back on and continuing to attempt to logon triggers rules with higher event thresholds.
- Persistent shutdown – The device will continue to shutdown when the Out of Contact and Unrecoverable timers expire, or until the device status is changed from Lost or Stolen to Found on the DataDefense Server and retrieved by the computer during a check-in event. The check-in event would be during a system boot and before the shutdown occurs again.

Destructive actions

- Secure delete files – Files are overwritten to permanently destroy the data on the hard disk, then the filename is removed. Each file is handled sequentially, first being overwritten, then deleted. You have the option to overwrite the file from one to eight times before the file is deleted.
- DOD delete files – This method of deleting files adheres to the DOD 5220.22-M standard of deleting data as specified in the National Industrial Security Program Operating Manual.

In setting up data destruction, it is important to consider speed versus time along with the risk factor. Assuming time is of the essence, you need to determine which information poses the greatest risk if compromised and deal with it first. After that, you can continue to destroy less sensitive data until there is nothing of importance remaining on the device.

DEVICE STATUS AND SETTINGS

All devices in the DataDefense environment have a status which indicates the current state of the computer. Prior to installation of the DataDefense Agent, the device's initial status is Provisioned. Once the agent has been installed on the device, the device status is automatically set to Active.

In addition to device status, each device has a set of parameters associated with Check-in Frequency, Out of Contact, and Unrecoverable. These values are initially specified during the provisioning process and can be modified at the device or group level. This section gives an overview of device status and device settings.

Device Status

When a device status is Active, it means that the DataDefense Agent has been installed and is checking in with the DataDefense Server regularly. If the computer is ever lost or stolen, you can change the device status with the DataDefense™ Admin Console so that actions are immediately initiated the next time the device connects to the internet.

Device Status can be set to:

- Active
- Lost
- Stolen
- Found
- Inactive

If a device is stolen, you can immediately send it a status change to minimize the amount of time your sensitive data is out of your control. When you change the device status to Stolen, you are prompted to select a set of actions to be performed the next time the device connects to the DataDefense Server through an internet connection (such as at System Boot). The action you select here overrides the existing set of rules assigned to this device and causes an immediate trigger of the action as soon as the device connects to the DataDefense Server via the internet.

If a device is lost, but it is unclear whether it has fallen into the wrong hands, you can set the status to Lost and select a set of actions that are less severe. The next time the device connects to the DataDefense Server those actions are downloaded to the device and are immediately triggered. An example is that if a device is lost, it might actually be in the hands of another authorized user (such as an IT employee or support person). By setting the status to Lost and triggering a message to be displayed, that person would have an opportunity to return the device to its owner before any data is destroyed.

When a device status is changed to Found, it will cancel any actions set under the Lost or Stolen status change. The Found status is similar to Active.

The Inactive status is used if you no longer need the DataDefense service on a particular device (for example, you are replacing the computer and have completely removed any sensitive information). In order to uninstall the DataDefense Agent, you first need to change the device status to Inactive.

The Uninstalled status is set automatically when the DataDefense Agent is uninstalled from an Inactive device. These are devices that are no longer managed by the DataDefense service. All devices with Inactive status should eventually move to Uninstalled status to finish the cycle. Uninstalled status is similar to Provisioned, in that, the status is automatically assigned and managed by the DataDefense service.

Device Settings

Many rules and actions are based on a period of time elapsing between certain events. There are standard check-in events such as startup, shutdown, login, logoff, lock, unlock, and creating a new network connection, where the device will automatically establish a connection and check in with the DataDefense Server. There are also periodic check-ins that happen while the device is online. At regular intervals, the DataDefense Agent will automatically establish a connection with the DataDefense Server and check for any rule or status changes since the last time it checked in. Check-in Frequency can be set to incremental values between 30 minutes and daily.

The Out of Contact setting allows a device to be offline (and not checking in) for a specified period of time (from one hour to one month). The Timer is a grace period that limits the amount of time the device can be used after exceeding the amount of time it has been Out of Contact. The important difference to remember between the two is that Out of Contact time is linear (based on a certain number of minutes from last check-in) and the Timer is based on cumulative uptime (the number of minutes the device is switched on).

An optional warning message is available to warn the user that the Timer is active. This message can be customized so that it makes sense to the owner of the device, but might be less alerting to a would-be thief.

The Unrecoverable setting specifies the amount of time that a device can be offline before it is considered permanently unrecoverable. The available settings time periods are in one month increments from one month to 12 months. Unrecoverable rules are activated when a device that has been offline or powered off for an extended period of time (past the time period selected) is turned on and not connected to the internet. Any rules that use the Unrecoverable parameters are then immediately executed, even if the user never attempts to login. The device will attempt to check-in with the server during the boot process and if the check-in fails, the Unrecoverable rules are processed.

Device Settings are assigned when a device is first provisioned. All devices being provisioned at the same time receive the device settings selected during the provisioning process. Device Settings can be modified on individual devices or by using a Group. When using a Group, changing the device setting will change the setting for all devices currently assigned to the Group. If you add a device to a Group later, it will retain its original device settings until they are changed by the administrator – either by directly modifying the device or by changing the device settings for the group.

TARGETING DATA WITH DATA SETS AND FILE LOCATIONS

In order to secure data on your devices, you first have to identify where the data resides on each device. The DataDefense solution has simplified this process by providing a standard set of data sets and file locations that are based on commonly used Microsoft Windows locations and document types.

There are generally two types of data sets: location-based and document-based. Location-based data sets assume that employees comply with standard practices and store documents in typical Windows locations such as My Documents and the Desktop folder. Document-based data sets assume that employees may save documents in locations other than the typical Windows locations. The standard file types associated with the type of document being targeted are sought out on all local drives.

In the case of encryption, the parent folder for each file is set to encrypt files, thereby, encrypting any files added to, or created in the folder. This approach ensures files created in these folders are immediately encrypted by the operating system. In general, both Document-based data sets and Location-based data sets can be used to encrypt files and/or delete files, however, there are a set of specifically designed data sets that will most efficiently handle the task of encryption and a set designed to optimize data destruction.

In addition to the built in data sets and standard locations, you can create customized data sets to suit the needs of your particular situation. If your company specifies that users keep important data in a particular location on their computer, such as C:\DATA\, you can create a data set that allows you to easily target data in that folder. You can also create data sets that are a combination of the built in data sets with your own customized settings added to it.

ALERTS AND RISK LEVEL

In addition to encryption and destruction, the DataDefense service provides several mechanisms for assessing risk, all of which are built around an exception management model. The primary purpose is to minimize administrative burden and allow the DataDefense administrator to focus their attention on devices at risk. This is accomplished by generating alerts, displaying a real-time risk-level indicator for each device, and providing charts which track activity for a variety of parameters.

Alerts provide an indication of risk related activity for all devices managed by the DataDefense service. From an information management perspective, alerts are grouped by device, providing a top-down view of all devices generating alerts, from which you to drill down to a specific device to get more detailed information, and ultimately, respond to the threat if needed.

Alerts are generated for the following events:

- New device is installed
- Rule threshold is exceeded
- Rules are executed by the client (e.g., Invalid Login)
- Device Status is changed (either by the Administrator or by the Timer expiring)

An Alert is generated when the threshold for a rule is exceeded. This is intended to immediately notify the administrator that something suspicious is happening on a particular device. If an alert is received for a device where the login attempt threshold has been exceeded, the administrator may want to proactively contact the device owner to check if they are having problems logging on, or if their device may have fallen into the wrong hands.

Note: The DataDefense Admin Console can also be configured to email alerts to the administrator(s), or to an email address designated by the administrator(s).

In addition to alerts, risk level is another method for providing feedback to the DataDefense administrator. Risk indicators are automatically escalated by the DataDefense service and are triggered by consecutive login failures or expiration of the Out of Contact and Unrecoverable time intervals. The DataDefense administrator can manually reset the risk level of a device if required.

There are three risk levels that a device can have:

- High: indicated by a Red dot on the Admin Console
- Medium: indicated by a Yellow dot
- Low: indicated by a Green dot

Risk levels are automatically escalated based on the following criteria:

- Green: normal operations, device check-ins are on time, and less than 2 sequential failed login attempts.
- Yellow: medium risk level is triggered by a 2nd failed sequential login attempt, device is late for check-in, or the Out of Contact interval has expired. Risk level will reset to green once the device checks in or when the user successfully logs in.
- Red: high risk level is triggered when the device status is set to Lost or Stolen, the Unrecoverable time period has elapsed, the Timer has elapsed, or when the 1st Invalid Login Rule has been triggered.

In addition to alerts and risk level, the DataDefense Admin Console provides several charts that provide historical information for a variety of parameters. The administrator can use the charts to tailor device settings and invalid logon rules.

- Check-in Freq (Histogram) – Displays a column chart depicting the number of devices having a particular Check-in frequency setting.

  Note: The Check-in Freq (Histogram) chart displays the current Check-in Frequency for all devices, therefore, it is not possible to filter the information by time period.
- Consecutive Failed Logons (Histogram) – Displays a column chart depicting the number of devices having failed logons in the range of 1 - 15.
- Failed Logons (per hour) – Displays a bar chart indicating the total number of failed logons for all devices on an hourly basis.
- Out of Contact (per day) – Displays a column chart indicating the total number of devices exceeding their Out of Contact setting on a daily basis.

PUTTING IT ALL TOGETHER – ENTERPRISE-CONTROLLED PC DATA SECURITY

Let's say an employee's laptop is stolen. The employee immediately calls you, the DataDefense administrator, and reports the theft.

You logon to the DataDefense Admin Console and change the device's status to Stolen, which instructs the device to destroy any sensitive data files immediately. As soon as the thief connects the device to a network, the DataDefense Agent checks in with the DataDefense Server, the device receives this instruction and the sensitive data is deleted by processing the Device is stolen rules resident on the device.

If the thief does NOT connect to a network and instead tries to login to access the data, after several failed attempts, the computer displays a message. After several more failed attempts, encryption keys are deleted, making encrypted files inaccessible. With subsequent failed attempts, additional files are deleted as specified by the rules you had set up.

If the thief is eventually successful at logging in before all of the data is destroyed, he still only has a limited amount of time before the Out of Contact and Timer periods expire and the remaining data is deleted.

If the thief decides to sell the device, either locally, or using a popular auction site, the Unrecoverable timer, in conjunction with Out of Contact, play an important part in securing the data from compromise. As the device moves from the thief to the purchaser, Unrecoverable continues to measure time. When the device is powered on, the DataDefense Agent will verify the time periods and if Unrecoverable has been exceeded, the rules are processed and the data is eliminated.

Once an action has occurred and sensitive data has been deleted, if possible, the DataDefense Agent will communicate its progress and status back to the DataDefense™ Server confirming what occurred.

EXAMPLE OF HOW DATA MIGHT BE DESTROYED:

Event	Rule Triggered	Action
1st Invalid Login	None	Nothing happens.
3rd Invalid Login	Failed Logons (3)	A message is displayed to the user advising them to contact the Help Desk.
6th Invalid Login	Failed Logons (6)	EFS Certificates are destroyed, rendering encrypted files unusable.
9th Invalid Login	Failed Logons (9)	Files in the user's account are deleted, as well as most other common types of files located on all local drives.
12th Invalid Login	Failed Logons (12)	Deletes the Communications folder and any remaining files across all local drives.
Device is not connected to the network		
Out of Contact expires		Timer activated then a message is displayed to the user.
Timer expires		EFS Certificates are destroyed, rendering encrypted files unusable. Device then goes into persistent shutdown.
Device is connected to the network		
Administrator sets status to Lost		DataDefense Client detects change in status. A message is displayed to the user, then all EFS Certificates are destroyed. Device then goes into persistent shutdown.
Administrator sets status to Stolen		DataDefense Client detects the change in status. All files in the user's account are deleted, as well as most other common types of files. Then the Communications folder, and any remaining files across all local drives, are deleted.

BENEFITS OF DATADEFENSE

Until now, business leaders have been forced to depend on end user compliance with corporate security policies to protect sensitive data. The DataDefense solution, offered by Iron Mountain removes the need for end user compliance and returns control and safeguarding of data to business leaders and owners.

The DataDefense™ service complements other data security solutions and works even when they fail. It protects sensitive data by encrypting and destroying it. It does not rely on only a single mechanism to protect your data, but instead uses multi-layered approach that is designed to detect and prevent a multitude of situations where your data could be compromised. It operates whether the computer is connected to the internet or offline. It cannot be disabled. It is transparent to the user and thus requires no training or special compliance. It is administered remotely, requiring minimal IT support.

- **Complete Security Solution To Prevent Unauthorized Data Use**
  DataDefense provides security and organizational control for data on lost or stolen PCs, even after the hardware is outside the organization's control.
- **Transparent to the User**
  Protection for PC data requires no special end user compliance, burden or training.
- **Easy for the Administrator**
  DataDefense is designed for rapid, remote deployment and straightforward monitoring and control.
- **Complete Multi-Layered Security**
  Neutralizes many different threat scenarios with a variety of detection capabilities and security actions.
- **Intelligent Data Encryption**
  Finds and encrypts all data on all local drives.
- **Data Elimination**
  Without DataDefense, data on lost or stolen computers is at risk forever.

APPENDIX A: INTEGRATING WITH ENTERPRISE DIRECTORY

Enterprise Directory is used to validate DataDefense administrators and to display contact information for employee devices. Integrating DataDefense with your enterprise directory provides the following benefits:

- Enables administrators to use their enterprise directory user ID and password for authentication.
- Prevents administrators from having access to the DataDefense Admin Console after reassignment or termination.
- Facilitates Account Lifecycle Management, since your accounts are based on your existing enterprise directory accounts.

Note: Install Secure Socket Layer (SSL) certificates on the enterprise directory server that will be read by the DataDefense server. Using SSL is strongly recommended to prevent unauthorized interception of user credentials.

Integration Process Overview

The process of integrating DataDefense with your enterprise directory includes the following:

- Configuring your firewall to permit the DataDefense service to access to your enterprise directory using Secure LDAP.
- Defining the settings for your enterprise directory in the DataDefense Admin Console, which includes mapping contact information fields to corresponding enterprise directory fields.

APPENDIX B: SECURE CLIENT/SERVER COMMUNICATIONS

Iron Mountain has taken multiple steps to ensure communications integrity and security between all components of the DataDefense service. The following presents a high-level overview of the communications methodology between the DataDefense Agent and DataDefense Server, presenting some, but not all, of the techniques to guarantee the integrity and security of the communications.

Communications Encrypted using Industry-Standard SSL 3.0 and VeriSign®

Communications between all components of the DataDefense service are encrypted using industry-standard Secure Sockets Layer (SSL) 3.0. The communications protocol used by the DataDefense service is XML over HTTPS. This industry-standard, secure communications protocol can be remapped using standard techniques to ensure firewall integrity and complies with existing security practices in place with in the organization.

The identity of the DataDefense Server is authenticated and validated by a VeriSign Class 3 (128-bit) certificate.

Communications Always Initiated by the DataDefense Agent

In order to limit possible attacks and prevent spoofing the DataDefense Server, the DataDefense Agent is always the first to initiate communications with the DataDefense Server. The DataDefense Server is not architected to initiate communications with the DataDefense Agent and if the DataDefense Agent were to receive unprompted communications from a server, the communications would be considered an attack on the device. However, such an attack would require detailed knowledge of the orchestration of a communications session between the DataDefense Server and DataDefense Agent, and the ability to analyze the encrypted communications by compromising the SSL 3.0 protocol.

DATADEFENSE AGENT AND SERVER AUTHENTICATE EACH OTHER

When the DataDefense Agent initiates a communications session with the DataDefense Server, the DataDefense Server must authenticate itself to the DataDefense Agent in order to establish a secure communications session between the DataDefense Agent and Server. Communications are authenticated and encrypted with Secure Sockets Layer 3.0 and the identity of the DataDefense Server is validated with a VeriSign Class 3 certificate.

Once the DataDefense Server's identity has been authenticated and a secure communications session has been established (XML over HTTPS), the DataDefense Agent and the device must be authenticated by the DataDefense Server. This is accomplished by verifying the unique Authentication ID for the device.

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**