

PC DATA PROTECTION SUITE



Complete PC Data Protection

IS YOUR COMPANY AT RISK FOR A DATA SECURITY BREACH? ASK YOURSELF THESE CRITICAL QUESTIONS:

- Do your company's policies and technologies ensure full compliance with new legislative requirements?
- Does your company rely on end-users to keep PC data secure?
- What will be the consequences and implications to the company's reputation and revenue from even a single data breach?
- Can the company control the data on a PC or laptop, even if it's lost or stolen?

DATA PROTECTION IS A TOP PRIORITY

Enterprise organizations face an enormous challenge when it comes to managing vast amounts of data. Two of the most critical challenges are data protection and data recovery. The risks are especially great when it comes to PCs and laptops that fall outside the protection of the enterprise's central data center. New federal, state, and international regulations now require that companies take stringent measures to secure private and personal data – or face serious consequences if a data breach occurs.

Total costs associated with even a single data breach event can reach into the hundreds of thousands of dollars, or even more. The company can face damaging legal liability, fines and penalties, loss of reputation, and even customer defection. With the stakes so high, the protection of sensitive data is now a top priority for company executives and IT managers. With more and more sensitive information residing on PCs and laptops, it's time to look carefully at your company's data security risk.

COMPREHENSIVE PROTECTION – DATA ELIMINATION & ENCRYPTION, DATA RECOVERY AND ENTERPRISE-LEVEL CONTROL.

The most commonly used data protection method is encryption. However, the only sure way to guarantee total PC data security is to actually eliminate compromised data when necessary. Should data be eliminated, it is also imperative that the enterprise provide rapid, reliable recovery of the data for continued productivity.

Iron Mountain's PC Data Protection Suite offers comprehensive enterprise-control over the PC data protection and recovery process, with complete endpoint security. The first line of protection is Iron Mountain's DataDefense™, which automatically detects and monitors threats, and can encrypt and ultimately eliminate data to prevent its compromise or misuse. The second measure is Iron Mountain's Connected® Backup for PC, the undisputed number-one solution for automatic backup and rapid recovery of business-critical and confidential data. This total solution offers the peace of mind that the company will always have control over distributed PC data, even if they lose control over the device.

EASY ENTERPRISE-LEVEL CONTROL

Both DataDefense and Connected Backup for PC are administered in-house for complete enterprise-level control of data stored on PCs, both inside and beyond company firewalls. All end-user compliance obligations are removed, returning the responsibility of safeguarding PC data to the enterprise and IT leaders. With minimal administrative resources, the enterprise can rapidly deploy and manage all PC Data Protection Suite capabilities. With centralized controls in place, all data security policies can be fully enforced, easily and automatically.

AUTOMATED, TRANSPARENT SOLUTION

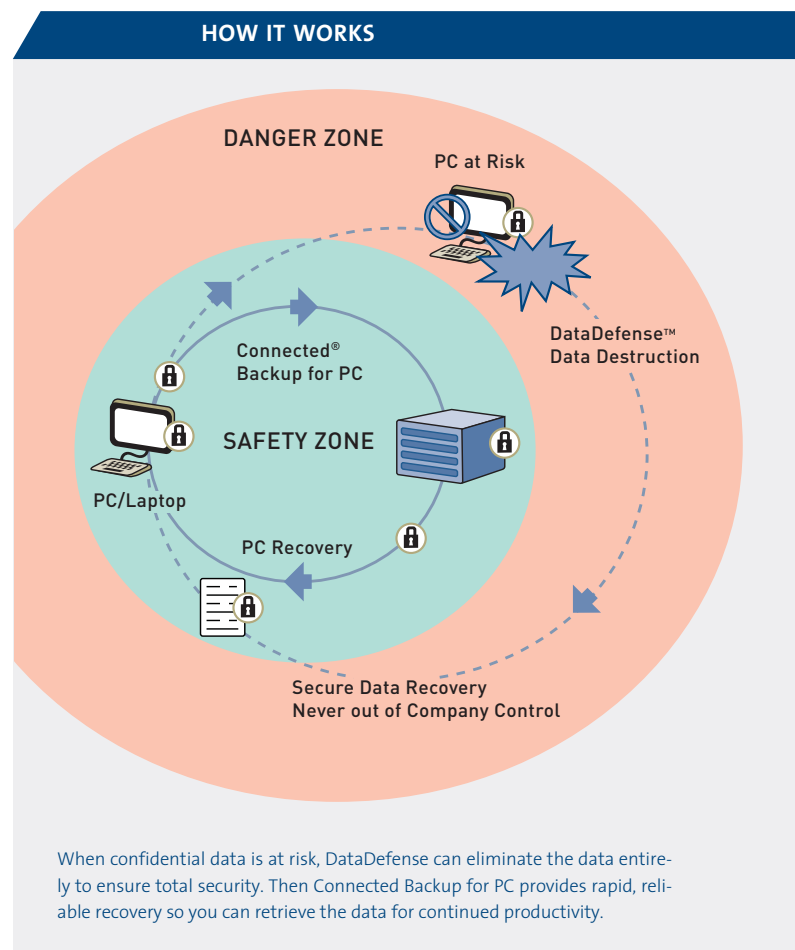
Data protection and recovery no longer need to be labor intensive jobs for your valuable IT resources or end-users. Iron Mountain's PC Data Protection Suite provides fully automated data protection, with no disruption of your organization's daily activities. With the combined power of both DataDefense and Connected Backup for PC, end-users remain productive, no matter what events threaten their data. The solution requires no special end-user compliance, training or change in their usual work processes.

ENDPOINT SECURITY

With the PC Data Protection Suite, IT administrators can choose to encrypt selected data, in any location on any local drive, and also destroy data when necessary. With DataDefense, the enterprise sets the criteria for threat detection, monitoring and actions to neutralize PC security threats. Connected Backup for PC also provides unbeatable security by using the highest levels of digital backup security available. 128-bit, Advanced Encryption Standard (AES) is used during transmission to the data center, for all data stored, and when users recover data.

With the PC Data Protection Suite, IT administrators can choose to encrypt selected data, in any location on any local drive, and also destroy data when necessary. DataDefense enables the enterprise to set the criteria for threat detection, monitoring, and actions to neutralize PC security threats.

IT retains control over the entire process, including setting backup timing, what types of data to back up, user access, and the storage impact of desktop and laptop data. Management of these centralized processes remains invisible to the end-user.



FLEXIBLE MANAGEMENT

DataDefense can anticipate a multitude of operational scenarios and suspicious user behaviors, and then take swift action to avoid a potential security breach. The enterprise can easily adjust threat monitoring and reaction rules to meet its unique PC data protection needs. For example, data destruction may be triggered based on the number of times an incorrect password is entered, or if a device is out of contact for a prescribed amount of time.

Connected Backup for PC enables equal flexibility. For example, the enterprise can set the timing for daily backups, determine which types of files are backed up and which are excluded, and set user access and functionality.

SUBSCRIPTION SERVICE OR LICENSED SOFTWARE

The PC Data Protection Suite can be delivered in two ways: Subscription service provides secure, off-site mirrored data storage, instant scalability and unmatched ease of use, and requires no capital investment. Licensed software allows organizations to run the solution inside their own IT environments. Delivery is from Iron Mountain or through partner providers.

KEY CONSIDERATIONS

THE COST OF A DATA BREACH

- Legal liability and lawsuits
- Non-compliance penalties
- Stock devaluation
- Damaging publicity
- Customer defection

COMPLIANCE REQUIREMENTS

- Gramm-Leach-Bliley (GLB)
- Sarbane Oxley (SOX)
- Health Information Portability and Accountability Act (HIPAA)
- 21 CFR part 11
- U.S. The Children's Online Privacy Protection Act (COPPA)
- California SB 1386 Identity Protection Bill
- State Laws Requiring Privacy and Security of Confidential Data
- The Family Educational Rights and Privacy Act (FERPA)
- EU Directive on Data Protection
- Personal Protection Law (Japan)
- Personal Information Protection and Electronic Documents (PIPEDA)

SOLUTION CRITERIA

- Comprehensive Data Protection
- Easy Enterprise Control
- Complete Administration
- Automated Transparent Solution
- End-User Transparency
- Endpoint Security
- Flexible Management