EVault®
A Seagate Company

The best case for the worst case.™

White Paper

Best Practices for Protecting Laptop Data

DISK-O-TAPE, INC.

Laptop Backup, Recovery, and Data Security: Protecting the Modern Mobile Workforce

Today's fast-growing highly mobile workforce is placing new demands on IT. As data growth increases, and that data increasingly finds its way onto laptops, the threats of data loss and security breaches have also increased. To guard corporate data on endpoints at all times, companies can follow a number of data protection and data security best practices. Incorporating these best practices can help you control sensitive information to mitigate the risk of regulatory and financial exposure and keep IT costs in check.

Phase 1: Define (or Update) Security Policies for Backup and Recovery on Endpoint Machines

If you have an existing endpoint security policy, revisit it to ensure endpoint data is protected throughout its lifecycle. If appropriate, include coverage of cloud-based backup and recovery services.

If you do not have an existing endpoint security policy, here are a few recommendations to get you started.

Audit Data

Identify critical information that flows from company servers to branch offices to endpoint devices such as workstations, laptops, and netbooks with hard drives. Begin your audit at the top of the organization, where strategy is devised and revenue is reported.

Audit accounting, sales, marketing, and support executives—the primary revenue generators and storage owners of critical data within the company. These groups are not only the most mobile teams within an organization, frequently taking work offsite, they are also the groups most often targeted for data theft because they carry sensitive client information. Their laptops may contain downloaded server files, email, instant messages, customer lists, sales and pipeline reports, strategy documents, financial reports, and even high-profile personal files.

Bottom line: Find out what is on those mobile devices.

Classify Data

Establish a scoring system to classify data based on its criticality. What would be the impact to the organization if the data were lost or stolen? Some organizations use a scoring range of 1 to 5—with 5 as the highest-ranked asset. Depending on the amount of data you need to protect, you may wish to simplify the scoring system to Restricted, Confidential, Internal Use, and Public.

From your information assessment, determine IT controls or actions to be enforced for each classification. These include access permissions, backup frequency, retention period, recovery requirements, and a disaster recovery plan in case of emergency. The outcome of this exercise should provide a baseline for your endpoint data protection policy.

Define Recovery Objectives

Once you have classified the data, the next step is to determine your tolerance for downtime and data loss. For each class of data, assign the following:

- Recovery Point Objective (RPO)—the tolerable period, after the last backup and prior to a failure, for which changed data may be lost
- Recovery Time Objective (RTO)—the tolerable period, after a failure, for systems and data to be restored to the recovery point

Be sure you consider the economic impact of not meeting these requirements. For example, a data breach that requires public notification not only subjects your organization to fines; the negative press coverage may also cause you to lose some current customers as well as scare away prospects.

Manage Policies

You should be able to manage endpoint security policies through a centralized console that provides granular control over the backup, recovery, and security capabilities that integrate with your existing infrastructure. If applicable, make sure your Macintosh computer users are covered too.

Configure and report on policies by device, user ID, user roles, and regulation. This will help you demonstrate due diligence of your endpoint protection program. Auditors will love it.

Inform Employees

Clearly define and communicate backup and data security policies to your staff. Explain how policies, backed by technology, will help specific users restore lost files and keep sensitive information out of the wrong hands.

Phase 2: Enforce Endpoint Controls

Once you have established the requirements for your endpoint data protection policy, Phase 2 describes controls for enforcing and sustaining your policy. Here are six focus areas to help you protect mobile laptops and automate enforcement.

Set Backup Policies

The first step is to make sure employee laptop data is properly protected. Set policies that match your recovery objectives. The backup solution should give you granular control over backup frequency and retention and enable you to configure policies by device, user ID, or user role. Back up your most critical data as frequently as every minute to ensure minimal data loss.

To minimize downtime, use a backup solution that works even when employees are offline. Cloud-connected™ backup solutions maintain a local cache on the laptop hard drive so restores can be performed locally—no network connection required. You should also have control over the size of the local cache.

Encrypt Data Stored on the Laptop Hard Drive: Whole Disk vs. File/Folder

The traditional method for securing laptop data is whole-disk encryption. Software installed on the device encrypts the applications, operating system, and disk all the way down to the hardware level. Whole-disk encryption usually requires that employees provide a password as soon as they turn on the device, known as a pre-boot authentication, and then a second separate password to authenticate to the operating system.

One downside of whole-disk encryption is that once the laptop is unlocked and the system is up and running, all the data on the device is unprotected. Other people using the laptop, or accessing the network through background processes (such as in malware) can access the at-rest data on the laptop.

Another downside is performance degradation. Encrypting and decrypting every piece of data takes time, which can slow down the machine and hurt employee efficiency.

Yet another downside is having to rely on your employees for a particular action. For example, some employees may not activate the boot-level password because they fear getting locked out of the system.

Data Encryption and Deduplication: Can They Happily Coexist?

Traditional data deduplication and encryption technologies are at odds with one another. Data encrypted with different encryption keys cannot be deduplicated. Essentially, you have to choose between investing in security or storage.

A workaround used by most backup vendors is to decrypt the data, deduplicate it, and then re-encrypt it. But this leaves your corporate data vulnerable while it’s unencrypted. Also, the key is shared and thus is equally vulnerable.

Another option is to perform data deduplication across encrypted data by sharing one key across all employees. But this makes the solution only as strong as a single key.

Only secure, automated key management makes it possible for encryption and data deduplication to work together. The best way to do this is to complete the encryption process up front and then run data deduplication on the encrypted data using a secure key escrow system. Since the data is encrypted before it is deduplicated, you gain the storage benefits of data deduplication along with the strong protection of multiple, cryptographically random encryption keys.

A final issue is deployment time. Whole-disk encryption solutions can be difficult to deploy, require significant setup time, and increase Help Desk call rates.

In contrast, file/folder encryption is more advanced and performance friendly. This flexible method encrypts data as it is stored on the laptop and decrypts it when an employee opens an application file. This greatly reduces the performance penalty. File/folder encryption also ensures that data is protected whether the laptop is on or off.

Equally important, file/folder encryption can be transparent to employees, eliminating the need for them to remember additional passwords to secure sensitive data on their laptops. This transparency will curtail employee resistance and minimize IT Help Desk calls requesting password changes.

Managing this approach is easy at the IT level, too. Deploying and supporting file/folder encryption is straightforward. IT administrators can use policy-based granularity to select specific files and folders to encrypt as employees use them on the laptop. By using automatic, policy-based enforcement instead of employee, behavior-based enforcement you gain much greater protection and security.

Prevent Data Leakage Through Port Access Control

Data leakage is the unauthorized transmission of data. Data can be leaked by attaching a storage device to the laptop's USB, serial, parallel, or FireWire (IEEE 1394) ports; writing to a CD or DVD; or even via a Bluetooth wireless connection.

First, define the read/write access permissions for the different ports on employees' laptops. This procedure is sometimes also called device control.

After you have set your device access control permissions, you can work on policies for protecting data in transit.

Enable Security for Backed-Up and Restored Data

Organizations seeking to protect data commonly overlook the data backup process. You first need to ensure data is encrypted before it leaves the laptop. Then you want to ensure the transmission is secure: A secure sockets layer (SSL) will take care of that. You have to do both to guarantee your corporate data is protected at both ends of the process. Finally, ensure the backup data remains encrypted while at rest in the vault.

Remotely Delete Data If the Laptop Is Lost or Stolen

It's estimated that in airports worldwide 800,000 laptops are lost or stolen each year. When this happens to your organization, the data on the laptop's hard drive should be destroyed, either on a command or using a timed "poison pill."

Ensure that your digital shredding mechanism prevents future data retrieval with disk recovery tools. It is a best practice to execute multiple deletes and "write overs," which will enable you to meet the most stringent government and industry regulations. This will eliminate data remanence—the possibility that some residual representation of data remains on the hard drive.

Employ Device Tracking to Retrieve Stolen PCs

Most organizations want to know where their company assets are and who may be accessing their data.

By enabling embedded device tracing capabilities, business owners, IT, and government officials can locate the mobile device once the device connects to the Internet. Such a mechanism can deter theft—few people steal mobile endpoints they know can be traced.

Phase 3: Ensure Employee Adoption

As with any corporate software solution, end user acceptance is essential for success. The more friction your employees experience, the more likely they will work around it. Conversely, the more friction-free the solution, the greater the adoption rate, which leads to better overall security for your company.

“Ease of use” and “security” don’t have to be at odds. There are a number of steps you can take to help increase employee acceptance of new backup and data security technology.

Eliminate Performance Constraints and Limit User Involvement

Choose a backup solution that will be as friction-free as possible—one that can be installed and updated silently, and runs automatically in the background, undetected by your employees. If they see performance degradation, employees will find a way to disable the software.

Enable User Independence

Empower your employees with a simple user interface for performing common operations. By streamlining the user experience and putting employees in control of their backup and restores, you will reduce Help Desk calls and take the pressure off of IT.

Phase 4: Keep IT Costs in Check

In a rush to mitigate the risk of data loss and exposure, many organizations have built a patchwork quilt of mobile backup and security solutions. This can prove costly to maintain and it can create holes in coverage that leave your organization vulnerable. Following these best practices can help you reduce IT costs and minimize overhead.

Centralize Management with an End-to-End Solution

Find an end-to-end solution that is easy to deploy, easy to configure, integrates with your existing desktop management infrastructure, and can manage all policies via a centralized console. You should have granular control over the backup and recovery and security features. This will save your staff loads of time.

Reduce Network Congestion

Bandwidth throttling and global source-side deduplication help reduce network congestion; they should be requirements for any laptop backup and recovery solution. Source-side deduplication means that only new and changed data blocks are sent during a backup cycle. Because mobile workers tend to download a lot of data, source-side deduplication should be global, a process that takes efficiency a step further. It compares changes to data blocks both chronologically (e.g., day-to-day edits to a Microsoft PowerPoint presentation) and horizontally (e.g., the same corporate presentation saved across all sales employees’ PCs).

Leverage the Cloud to Minimize Overhead

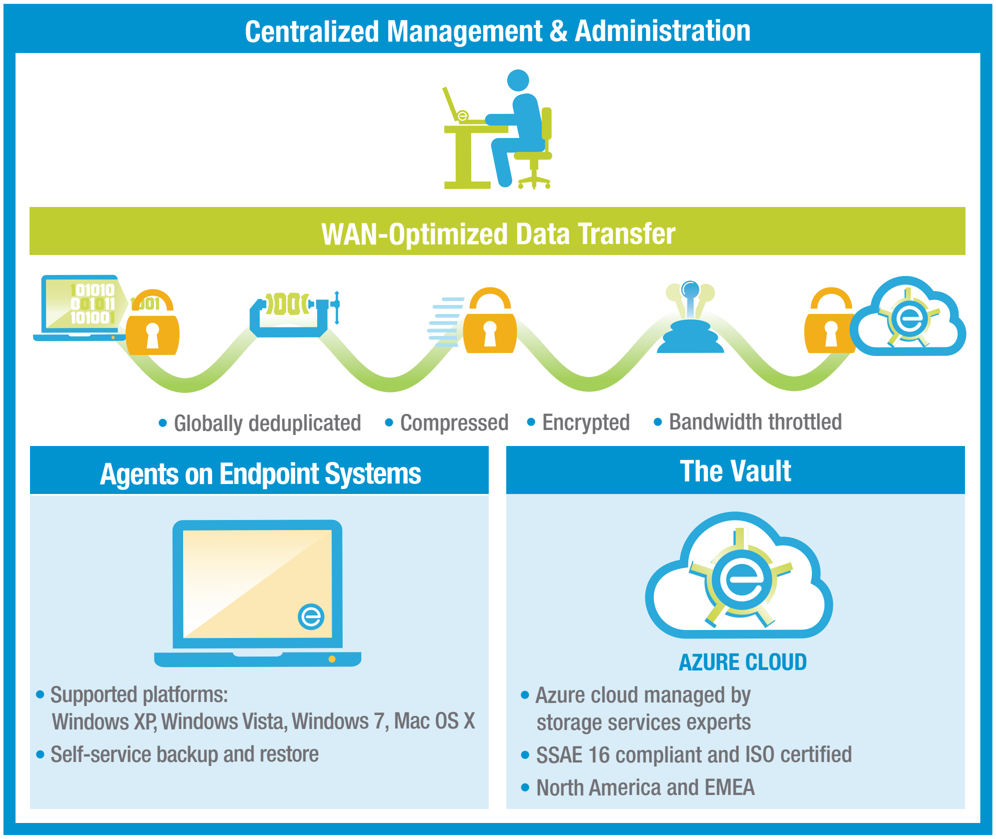
Driven by less-expensive bandwidth, proven security protocols, and growing cultural acceptance of cloud business models, organizations are increasingly turning to cloud services for simpler, more scalable, and more cost-effective methods of storing business-critical information. Because cloud services offload the IT department's responsibility for purchasing and maintaining software, hardware and storage, IT enjoys seamless scalability and can respond with greater agility to changing requirements.

But sending data offsite to a third party isn't without its risks. You have to make sure the proper security and redundancy measures are in place. Data should be encrypted as it travels over the wire and remain encrypted in the cloud. There should be no back-door decryption keys: Only your organization's key holder should have the correct code. What's more, the cloud vendor should be SAS 70 Type II certified, which attests to an organization's ability to audit and maintain its internal management controls over a period of at least six months.

EVault Endpoint Protection: Built on Best Practices

EVault® Endpoint Protection integrates PC backup, recovery, and data security capabilities so you can control valuable data across your mobile workforce today.

HOW IT WORKS



Centralized Management & Administration

WAN-Optimized Data Transfer

- Globally deduplicated
- Compressed
- Encrypted
- Bandwidth throttled

Agents on Endpoint Systems

- Supported platforms:
  Windows XP, Windows Vista, Windows 7, Mac OS X
- Self-service backup and restore

The Vault

AZURE CLOUD

- Azure cloud managed by storage services experts
- SSAE 16 compliant and ISO certified
- North America and EMEA

The company locks down endpoint data.

- Disk encryption and port access control keep data safe
- Remote data deletion wipes data clean
- TCP/IP device tracing tracks down missing PCs

Users get worry-free backup and self-service recovery.

- Silent, unobtrusive backups that are automated and continuous
- Simple interface so end users can back up and restore without involving the Help Desk
- Cloud-connected with data stored in a local cache and moved offsite for disaster recovery

IT gets more oversight with less overhead.

- Centralized, policy-based administration makes it easy on your staff
- No data block is backed up twice so it's easy on your network
- Cloud deployment makes it easy on your infrastructure

EVault Endpoint Protection enables your IT department to control corporate data assets and meet regulatory requirements while enabling your company's mobile employees to be as productive and effective as possible.

Take the Next Step

To learn more about EVault backup and recovery services,
contact Disk-O-Tape, Inc. by phone at 800-923-8273 or 216-765-8273,
or email at evault@disk-o-tape.com, or visit www.disk-o-tape.com