Enterprise Laptop, Desktop Backup and Recovery Considerations

Whitepaper

This whitepaper examines key considerations for Enterprise laptop, desktop backup and recovery, with special emphasis on distributed environments with remote and mobile users.
This whitepaper also provides information about how Copiun Data Manager delivers a scalable, easy to manage and easy to use solution designed for distributed enterprise environments with remote and mobile users.

August 2010
Copiun Inc
www.copiun.com

Table of Contents

INTRODUCTION

There are several studies indicating that as much as 50% of corporate data resides on PCs distributed within the company. Notebooks and mobile PCs now account for 50% of installed PCs and majority of new PC purchases (Gartner). When you consider that a staggering 12,000 laptops are lost every week on airports in US alone (Ponemon Institute) – it becomes clear that this corporate data is at risk of loss. When you take into account that on average it costs $3,957 for every data loss incident (Pepperdine University), it underlines the need for having a reliable and cost-effective backup and recovery solution for PCs.

Traditional methods of asking users to manually backup their PC data to network shares doesn't work anymore, because users are increasingly working remote and disconnected, where the opportunities for backup are few and far between. Ironically, it's these users who are the most vulnerable to data loss because they are mobile. As a result, there is increasing risk that end users are taking matters in their own hands. They are performing do-it-yourself backups to personal USB drives or signing up for consumer cloud based backup solutions (SearchDataBackup) – putting confidential company data on non-IT assets and potentially running companies afoul of regulatory requirements.

According to recent reports less than 40% of IT organizations have formal processes in place for backing up PCs (Enterprise Strategy Group). This is partly because until now there has been a dearth of viable enterprise options (Gartner). However, IT organizations continue to be challenged with endpoint protection and are looking for solutions: in a recent ESG survey, respondents ranked desktop/laptop backup as their #4 data protection challenge and spending priority.

This whitepaper describes key considerations to take into account while evaluating a backup and recovery solution for the desktops and laptops in your organization, with a special emphasis on the following areas:

a) Deployment, administration and reporting requirements
b) Distributed and mobile user requirements
c) End user requirements
d) Data De-duplication requirements
e) Security requirements
f) Beyond backup – how to derive operational value from your backup and recovery solution

This whitepaper also looks at Copiun Data Manager and its capabilities vis-à-vis the above requirements.

KEY CONSIDERATIONS FOR ENTERPRISE CLASS PC BACKUP AND RECOVERY

While evaluating an enterprise PC backup and recovery solution there are several factors to consider:

Ease of Administration, Deployment and Reporting

Ease of administration, i.e. ensuring reliability and desired service level without undue burden is key; especially when managing data on PCs, because of their sheer number and because PCs are perhaps the most volatile piece of IT infrastructure in the company as they can shutdown or lose connectivity at any time. Look for the following specific requirements:

1. **Service level based management**: In a PC environment, there are a lot of environmental errors (shutdown, loss of connectivity etc) – which can cause backups to fail. Most of these errors are false negative errors that don't need attention. However, frequently there are also real errors which can get lost in the daily noise of false negative errors. Look for a solution that can automatically identify and handle these false negatives by letting you define a Service Level and can then automatically manage it – thereby only escalating real problems to you.
2. **Ability to group machines into logical groups**: When you're managing a large number of systems, it is important to be able to group them. You may want to group the PCs you're managing by functional groups or physical location or some other criteria. Look for a solution that lets you organize PCs into multiple groups for ease of management.
3. **Policy based interface**: When you're managing a large number of PCs, having an easy policy based interface that can allow you to centrally configure settings is really important. Look for the following capabilities:
    a. **Ability to create multiple policies**: In an enterprise, there are multiple groups, many with different needs for backup. For example, you may want to backup pictures and videos for your Marketing group, but not for the general population. Look for a solution that allows you to create policies according to your needs which can then be applied to entire groups of PCs, so you don't have to perform per-PC configuration steps.
    b. **Ability to specify what to backup and what to exclude**: Look for a solution that lets you specify what data to backup and equally importantly, what NOT to backup. Look for capabilities to include and exclude data based on folder names, file names and file extensions.
4. **Reporting**: Every product has some level of reporting, but specifically look for the following:
    a. **Dashboard**: a summary dashboard that tells you the key performance indicators at-a-glance so you immediately know which areas need your attention.
    b. **Daily email**: look for the capability that the backup product can send a daily status email to you so you don't have to login to the product every day to check the status.
    c. **Detailed reporting of key areas**: service level, backup status, recoverability status, storage usage, important events
    d. **Self-monitoring system**: Look for a system that manages its vital health indicators and alerts you whenever there is an issue that needs administrative attention.

5. **No schedule management**: Managing backup schedules across a large number of PCs is not only cumbersome, but is also error-prone. In any organization, PCs enter and leave all the time. It is nearly impossible to manually keep the backup schedule optimized in light of the volatile nature of the PC population – leading to backup server and network overload. Therefore, look for a solution that can auto balance backup schedules on an ongoing basis.
6. **Self-service recovery**: Look for a solution that allows end users to recover their own files, so they don't call the helpdesk for recovering their files.
7. **Ease of installation on the PC**: Look for a solution that can be pushed out via standard tools for purposes of installation and doesn't require any end user action for configuration. Some solutions require end users to either configure backup specification or license files – doing so across a large end user population is error-prone and burdensome and should not be needed.
8. **Ease of PC SW update**: Look for the capability to centrally update the PC software in an automated fashion without requiring user involvement. Also, look for the ability to test updates on a subset of machine before you update all the machines.
9. **Easy recovery for authorized administrative users**: There are situations when, despite the availability of self-service recovery, the administrator must recover the data for a PC. For example: during a laptop rebuild or for placing a legal hold on the PC data. Some solutions require cumbersome steps like logging in with end user credentials (a security and audit red flag!) and encryption keys before an administrator can perform the recovery. Look for a solution that permits authorized administrators to recover data in a simple way by authorizing against their Active Directory credentials.
10. **Automation of recoverability testing**: The old joke in backup is that backup was good, but recovery failed! Sadly, this is only too true as most backup solutions just focus on backup and put the burden of ensuring recoverability on the administrator. Look for a solution that automatically tests your backups for recoverability and provides you with a report, so when the CIO asks if the data is recoverable you can say YES with confidence!
11. **Easy remote troubleshooting**: Look for a capability to troubleshoot the backup agent on the PC remotely, i.e. being able to remotely view the diagnostic logs and change any configuration settings, if needed.

Storage and Bandwidth Efficiency

Across the entire PC population in a company, there is a lot of duplicate data. For example, identical files, or PowerPoint presentations using the same slides or PST files with the same message attachment. The ability to identify this common data and to transmit and store only unique data is crucial to deploying a cost-effective and scalable solution. The industry jargon for this capability is data de-duplication or dedup, in short. There are several types of data de-duplication approaches available in the market. But broadly, it can be classified along two broad axes: Dedup approach/algorithm and where the dedup is performed. Both are important to evaluate.

1. **Data de-duplication approach/algorithm**: Dedup approach determines how common objects are identified. This is the first step in every dedup process and is perhaps the most important one because

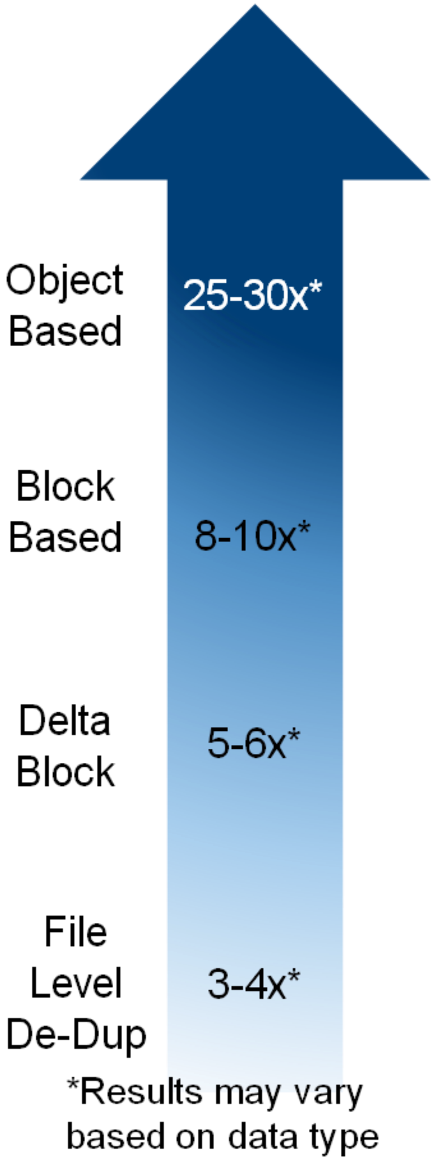
the better the approach to identify duplicate data, the more the dedup efficiency. Broadly speaking, there are 4 approaches to how duplicate data is identified:

a. **File-level**: This the most basic form of de-duplication, which can identify identical files and store them only once. The downside is that if you change the file by even a single byte, the entire file needs to be stored again.

b. **Delta-block**: Delta block technologies can identify changes to an already backed up document and backup only those changes. The downside is that if you save the file with a different name, the entire file needs to be backed up again, so while it is better than purely file-level de-duplication, it is still pretty basic.

c. **Block level**: Block level de-duplication breaks the file into fixed sized blocks and only backs up unique blocks. While better than file-level and delta-block technologies, this approach is best suited for database type stores whose physical block layout doesn't change. However, for document type data – most prevalent on PCs – where a simple save can completely alter the layout of the document, block level de-duplication isn't very effective.

d. **Object-based**: Object-based data de-duplication is the current state of the art and is the most effective solution for detecting duplicate data, even when physical block layout changes. Unlike block based technologies, object-based de-duplication is "content aware" and chunks the file into well known logical objects like slides, images, paragraphs, worksheets, attachments etc. The advantage is that even if the physical layout of a file changes – which can happen with a simple save operation – the logical objects can still be detected and stored only once. As a result, object-based de-duplication provides the best de-duplication efficiency for PC data with as much as 5-10x better performance vs. block based de-duplication.



2. **Where is the dedup performed**: Where the dedup is performed is crucial for WAN efficiency, which is critical if you have a large number of laptops or remote users. Look for a solution that has global or source-based de-duplication, so only unique data is sent over the network. Broadly, the following approaches are available:

   a. **Target based de-duplication**: In Target based de-duplication approach, the entire data is sent over the network to a storage device which then identifies duplicated data using one of the approaches described above and stores only unique data. This approach is the least network efficient and should be avoided for PCs.

b. **Source based de-duplication**: In only source-based de-duplication, the PC would identify duplicate data on the PC and only send data that is unique on the PC to the server. However, if there are other PCs with similar common data, they will store the duplicate data again on the server. This approach can suffice for a small number of PCs, but should be avoided for large numbers of PCs as it results in too much duplicate data to be stored.
c. **Global de-duplication**: Global de-duplication combines the best of source and target based de-duplication. The source machine – in conjunction with the server – identifies duplicate data across the entire company and as a result only data that is truly unique is transmitted and stored. This approach is the most WAN and Storage efficient and is also the most scalable approach.

Key Considerations for Remote and Mobile Users

Most organizations have an increasing number of remote and mobile users: an estimated 40% of US working population can work from home at least part of the time (Wikipedia), so ensuring secure and ongoing protection of these users is critical. Look for the following specific capabilities:

1. **WAN efficient**: WAN efficiency is critical, because transmitting too much data on already saturated links adversely impacts end user experience and further clogs your already saturated links. Look for a solution that has Global de-duplication as described in the previous section.
2. **Remote users who don’t frequently VPN**: An increasing trend is the mobile worker who doesn’t frequently VPN into the corporate network. Imagine a sales person who accesses their CRM from Salesforce.com and their email over webmail or Outlook 2007’s VPN-less support. Sometimes weeks go by before they VPN in to the corporate network. In many ways, these users are perhaps the most vulnerable to data loss because their data is likely only stored on their PCs. Look for a solution that can protect the data for these even if they don’t VPN in, without requiring your backup server to be hosted outside the firewall or opening incoming firewall ports.
3. **Disconnected backup**: Unlike servers, PCs can be disconnected from the corporate network at the time of backup. A backup solution that only works at scheduled time or event will have poor backup coverage because the PCs may be frequently disconnected from the network at the time of backup.
4. **Acceptable RTO for multiple sites**: If you have several sites that have a significant number of users, you need to pay special attention to the amount of time it takes to perform recoveries for users in those sites, especially full system recoveries. Having a single backup source is great from management perspective, but if that is the only source for recoveries the recovery time for your remote sites is going to suffer, because all recoveries will need to transmit data over the WAN, severely impacting the amount of downtime. Look for a solution that while providing for the central backup repository, also allows for distributed recovery sources to mimic your organizational footprint.
5. **Seeding the first backup**: If you have several sites with a large number of users, you may find that the first backup of the remote users over the WAN may take a long time. Look for a solution that provides

an option to "seed" the first backup via a portable piece of storage that can be shipped between sites, so you don't have to transmit a large amount of data over the WAN for the first backup.

Security

Security is obviously critical for any solution that manages your corporate data. Look for the following specific attributes:

1. **Encryption**: Any solution you evaluate should encrypt all at-rest and in-motion data with a minimum of AES 128-bit encryption. Avoid products that have "private" or "home-grown" encryption.
2. **Server location behind the firewall**: Avoid solutions that require that you place your server outside the firewall in order to protect remote users who are not connected via VPN. Even with encryption, putting a server with all your corporate data outside the firewall – where it is vulnerable to attacks from hackers – is a recipe for trouble.
3. **No need to open incoming firewall ports**: Avoid solutions that require you to open incoming firewall ports in order to protect remote users who are not connected via VPN. Similar to the previous point, this unduly exposes your data to the risk of attack from hackers.
4. **Active directory integration**: Ensure that the solution you are evaluating is integrated into Active Directory and does not require you to create a new set of username and passwords for your users to remember and your IT group to manage.
5. **Audit logs**: A centralized backup solution is great from the perspective of recoverability, but it poses some new security challenges. For example, a rogue administrator can access sensitive data from the CFO's laptop via the backup server. Ensuring that such attempts are recorded is important from a security and audit perspective. Look for a solution that keeps an audit log for all data access and recovery operations.

End User Ease of Use

It's critical that any solution that will be used by a large number of users be easy to use and non-intrusive. Anything that requires training will dramatically increase the cost of both initial deployment and ongoing maintenance as users will often forget what to do and call the helpdesk. Also, if the PC based agent is intrusive, it will most likely be disabled by the end user or they'll call the helpdesk to complain.

1. **Non-intrusive**: Ensure that the PC agent becomes and remains passive while the user is using the PC. Ignore any claims regarding CPU based throttling, since CPU usage based throttling is usually meaningless for the PC. This is because on most PCs, disk access is the biggest bottleneck as the disk is the slowest component amongst CPU, memory and disk. While the user is using the PC, if a program like the Anti-Virus agent or a backup agent starts reading the disk – it will bring the entire system to a crawl. Since a backup agent must access the disk, the best time to do so is when the user is not using the PC. Therefore, look for an agent that can detect whether the PC is in use, before it accesses any system resources. More details available here.

2. **Ease of use**: Look for an agent that doesn't require any end user training. Ideally, this means the following:
    a. **No user action required**: There should be no user action needed for initial configuration or ongoing maintenance of the product. More details available here.
    b. **No new interface for end users to learn**: Any application that introduces a new interface on the PC will likely require end user training. This is usually expensive and the problem is that the users often forget. Look for a solution that integrates into existing end user tools like Windows Explorer and Search so they require no end user training.
3. **Self-service recovery**: Ensure that the product allows end users to recover their own files. The user interface for recovery matters a great deal, because it needs to be used by non-technical end users, so pay special attention to that. Ideally, look for a solution that supports the following:
    a. **Full-text search integrated into Windows**: When end users can't find their files, they will likely search for it in Windows. Look for a product that can integrate into that workflow and allow users to access/recover their file as part of that workflow for the best end user recovery experience.
    b. **Browse support for the backup catalog**: Sometimes, there is a need to browse the backup catalog. Look for a product that provides easy browsing of the backup catalog via one of the standard user tools like Windows Explorer for the best end user experience.

Beyond Backup

After you've vetted a product against your requirements for backup and recovery, look for these additional requirements to satisfy day-to-day operational needs around data management.

1. **Access data from anywhere**: These days, most users have a Smartphone in addition to their PC and they often want to access their PC data from the Smartphone when they're traveling. Look for a solution that allows easy and secure data access from a Smartphone as an option, so if your corporate security policy permits it, you can enable such access.
2. **Federated search**: Many times whether for E-Discovery or for other internal forensics needs, there is a need to perform a search across the entire PC data or for a subset of users. Look for a solution that can satisfy those needs from the backup repository, so you don't have to manually gather data from each user's PC.
3. **Rapid risk assessment in case of stolen laptops:** When a laptop gets stolen, the first question everyone wants to get answered is: "what was on it"? Look for a solution that can quickly provide a searchable catalog of the entire laptop data so rapid risk assessment can be performed.
4. **Data migration:** A backup solution can be a great source to satisfy the data migration use case if it can support fast recovery speeds. For example, in case of a PC lease renewal situation, instead of manually copying the data from the PC, the backup application can be used for the data movement.

COPIUN DATA MANAGER

Copiun Data Manager is an enterprise class data management solution that enables IT organizations to regain control of corporate data on PCs, by providing: backup and recovery, risk assessment, federated search and lifecycle management for the entire PC population within the company. Following are the key attributes of Copiun Data Manager (CDM):

a) Up to 95% Storage and Bandwidth reduction via Global, Object Based data de-duplication
b) Designed for distributed sites and mobile users
c) Native End User Experience requiring no end-user training
d) Service Level based Management
e) Centralized, Policy based management
f) Security

Up to 95% Storage and Bandwidth Savings

Copiun's Object Based data de-duplication is performed at a global level and drives significant storage and bandwidth savings that are demonstrably superior when compared to any block or file level data de-duplication solution.

Object-based data de-duplication

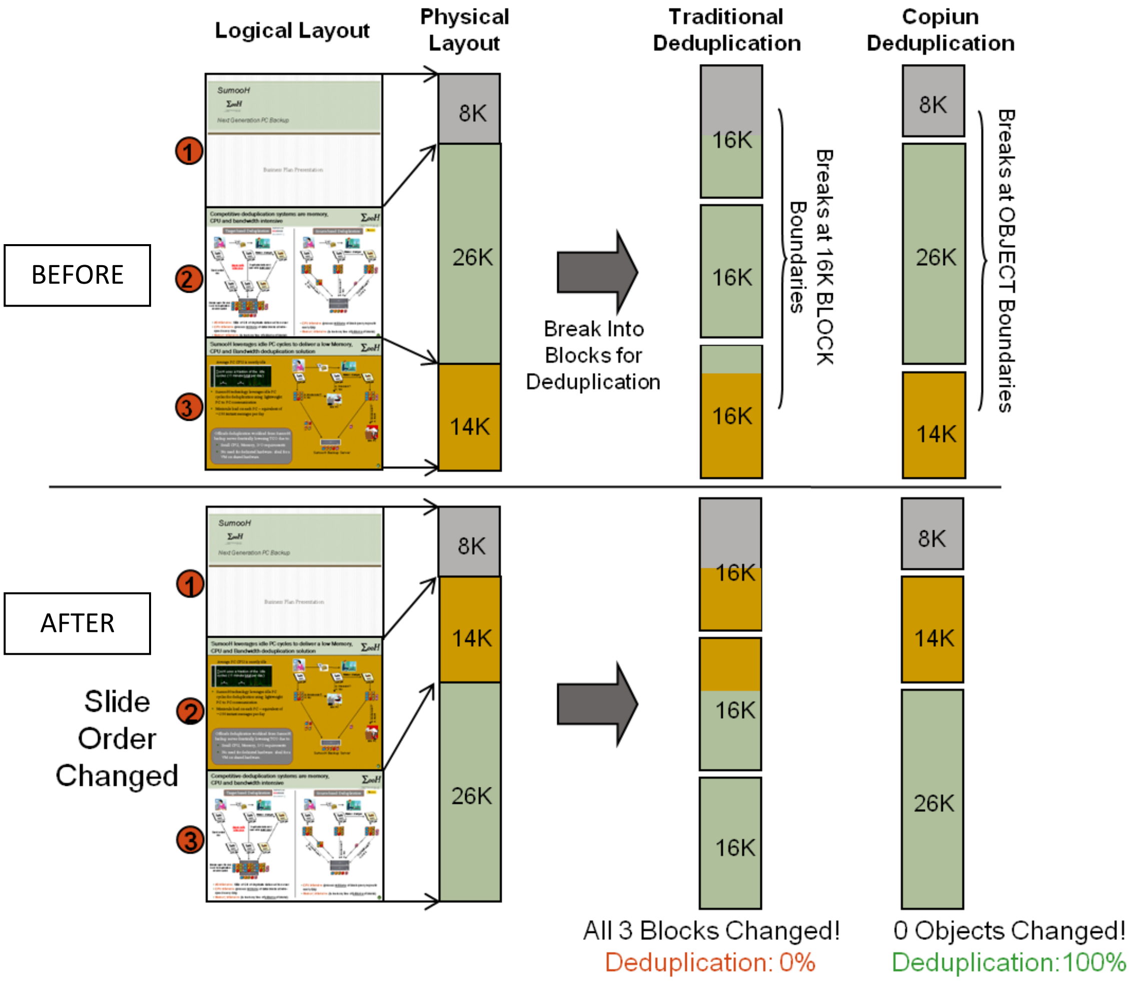
Copiun Data Manager (CDM) uses patent-pending Object-based data de-duplication, which can detect embedded common objects across unrelated files anywhere in the company. Copiun's object-based de-duplication "chunks" each file it processes into native objects like: images, slides, templates, paragraphs, worksheets, attachments etc. In the process, Copiun removes any metadata associated with those objects like position information – uncovering the logical object in its native form. This allows Copiun to identify a logical object anywhere, regardless of its location and only store and transmit it once per file type. This provides dramatically better savings than block-level data de-duplication for both the first backup and the subsequent forever incremental backups:

First Backup Savings

Imagine a million documents spread on thousands of PCs across multiple sites in the entire company. There are millions of common sub-objects like company logos, slides, worksheets, email attachments, etc. that are embedded in those files – all at different physical locations within those files. For example, the same image could be on slide 2 of one presentation and slide 3 in another one. Block-level de-duplication, which is oblivious of file formats, simply fails to detect those common objects because it can only detect common data that occurs at the same physical location. Copiun's object-based de-duplication can detect these sub-objects across millions of files – regardless of their location, and store and transmit them only once – providing tremendous savings as part of the first backup itself.

Forever Incremental Backups' Savings

Once the first backup has been done, Copiun does forever incremental backups, only backing up data that is truly new. Again, object-based data de-duplication provides tremendous savings on a day to day basis for the forever incremental backups. This is best illustrated by the following example:

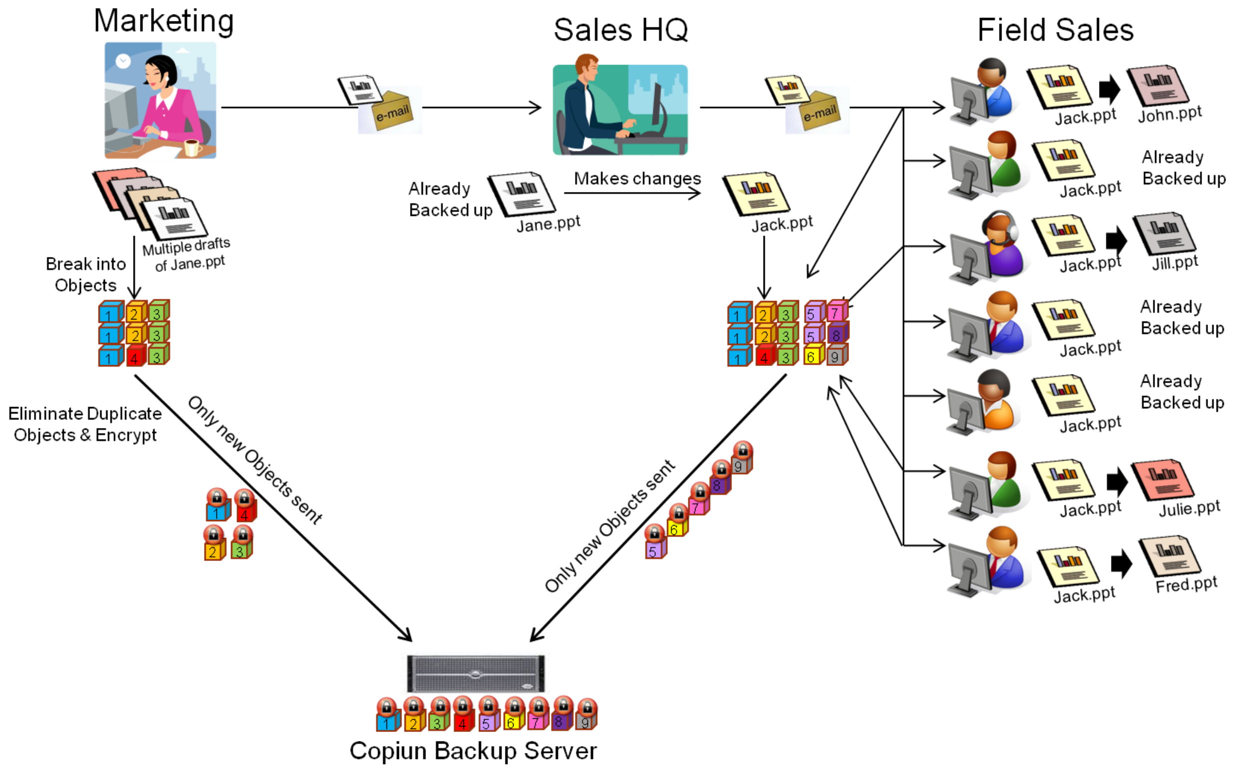


This is an example of a PowerPoint presentation with 3 slides. Shown here are the logical and physical layout of the 3 slides which are all of different sizes. A block-based data de-duplication solution would break the file at fixed block boundaries, in this case 3 equal sized blocks of 16K each. Copiun on the other hand will chunk the file at object boundaries, which results in 3 objects of different sizes each corresponding to one slide. The difference between the two approaches becomes apparent, as soon as there is a change that causes physical data layout change. Data layout changes are the Achilles' heel of block based data de-duplication, because even a small layout change can render block based de-duplication algorithms ineffective.

Let's say, the slide order is changed, slide 3 and slide 2 interchange their position, which causes the physical layout of the data in the presentation to change. A block based de-duplication solution would again break the file at 16K boundaries, but will fail to find any duplicate blocks – resulting in a 0% de-duplication. Copiun, on the other hand, will correctly chunk the file at object boundaries again and find the same objects, just in a different order – as a result achieving nearly 100% de-duplication with the only changes being backed up due to the metadata that has changed.

Global Data De-duplication

Copiun is designed from the ground up to use Global data de-duplication. Each machine – in conjunction with the CDM server – identifies duplicate data BEFORE it is sent over the wire. As a result only data that is truly unique is transmitted and stored – providing for the best WAN efficiency and also a scalable backup server.



Designed for Distributed Sites and Mobile Users

Copiun is designed from the ground up for distributed sites and mobile users. Copiun's global de-duplication provides WAN efficiency as noted above. Copiun's focus on the following key requirements makes it the solution of choice for mobile users and distributed sites:

Secure, nearly continuous backup for mobile users with or without VPN:

Out of the box, Copiun provides, secure, nearly continuous backup for mobile users as soon as they connect over the VPN. Unlike traditional solutions, there is no requirement for the user to connect to the corporate network at specified times. Instead, the backup automatically happens whenever the users connect to the corporate network via VPN, ensuring ongoing coverage.

Backup for remote users without VPN: Increasingly, remote users are only connecting to the corporate network via VPN intermittently. During that time, they have data on their PCs which is lying unprotected. Copiun's Constant Access Gateway option allows IT to ensure that secure backups for such remote users can happen to the Copiun server behind the firewall as soon as they connect to the Internet. Constant Access Gateway allows this to happen without requiring you to either place the backup server outside the firewall, or open any incoming ports within the firewall.

Since all data is encrypted using AES 128-bit encryption, the backup server is secure behind the firewall and no incoming ports are opened, this provides a secure way to backup your mobile users who are perhaps the most vulnerable to data loss.

Acceptable RTO for remote sites

As noted previously, if you have remote sites with a large number of users, ensuring an acceptable RTO with a completely centralized backup solution can be a challenge because all data needs to be recovered over the WAN. Copiun, while providing all the benefits of a centralized backup solution, also provides an option for Cache Servers for your large remote sites to provide LAN speeds for all recoveries done within that site. The Cache Servers are centrally configured from the CDM Server console and are self-managing. There is no requirement for ongoing storage management or backup of the Cache Servers. Additionally, the Cache Servers can be added or removed from the system at any time without requiring any downtime.

Seeding of first backup

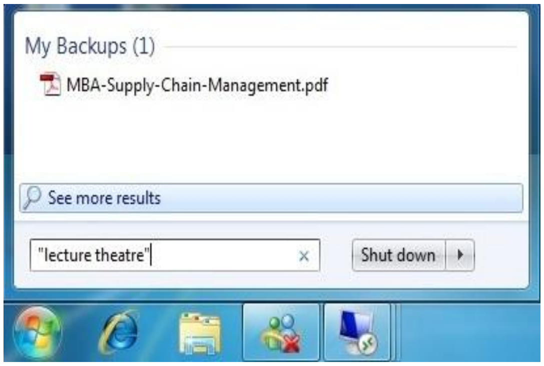
The first backup over the WAN for a large remote site can take significant time. To speed up the process, Copiun provides a "Seeding Server" option, which is a portable storage device that can be shipped to a remote site so the first backup can be done over the LAN to the Seeding Server. Since all data on the Seeding Server is encrypted, it can be shipped back to the main site, where it can be used to upload the data to the main server – thus obviating any need to transfer the first backup over the WAN. Once the first backup has been uploaded, subsequent forever incremental backups can easily be completed over the WAN.

Native End User Experience

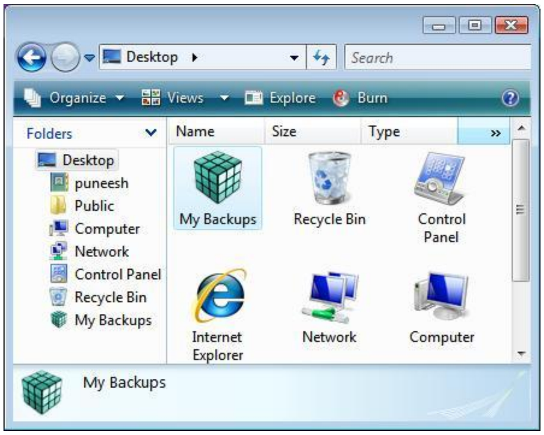
Copiun's design philosophy is to not have any new interface or application that IT has to teach their end users, because teaching anything new to a large number of end users is expensive and disruptive. This has led to a fully native end user experience allowing end users to take advantage of the full benefits of Copiun from their familiar tools like: Windows Search and Windows Explorer. There is no other application that they have to learn.

Full-text search based self-service recovery

Users on Windows 7 and Windows Vista recover their files using full-text search capabilities built into Windows. For example, let's say you are looking for a document that you created a month ago, which unbeknownst to you somehow got overwritten or deleted. If you perform a full-text search for content from that document using the search option in the Windows Start menu, your search results will automatically show matching results from the backup catalog – enabling end users to recover their data without having to learn anything new or going to a different application. Click here to watch a video of full-text search based recovery.



On Windows XP (also on Vista and Windows 7), there is a virtual folder called “My Backups”, which allows end users to recover their data by simply browsing through the folders, exactly as they would browse through My Computer or My Documents.



No end user configuration required

Copiun does not require any end user action or configuration to backup their data. The administrator simply configures a policy on the administration console and authorized PCs data starts getting backed up. If so desired, IT can provide power users to ability to “tweak” the backup policy configured for their PC – providing flexibility.

Non-intrusive agent

Copiun’s PC agent is designed to be invisible to the user. It detects whether the PC is in use, and remains passive while it is being used. Backups are only performed when the PC is idle, i.e. there is no keyboard or mouse movement.

Centralized Policy Interface

Copiun is designed to allow a single administrator to configure and manage a large number of PCs across multiple functional groups and sites.

Flexible policy interface

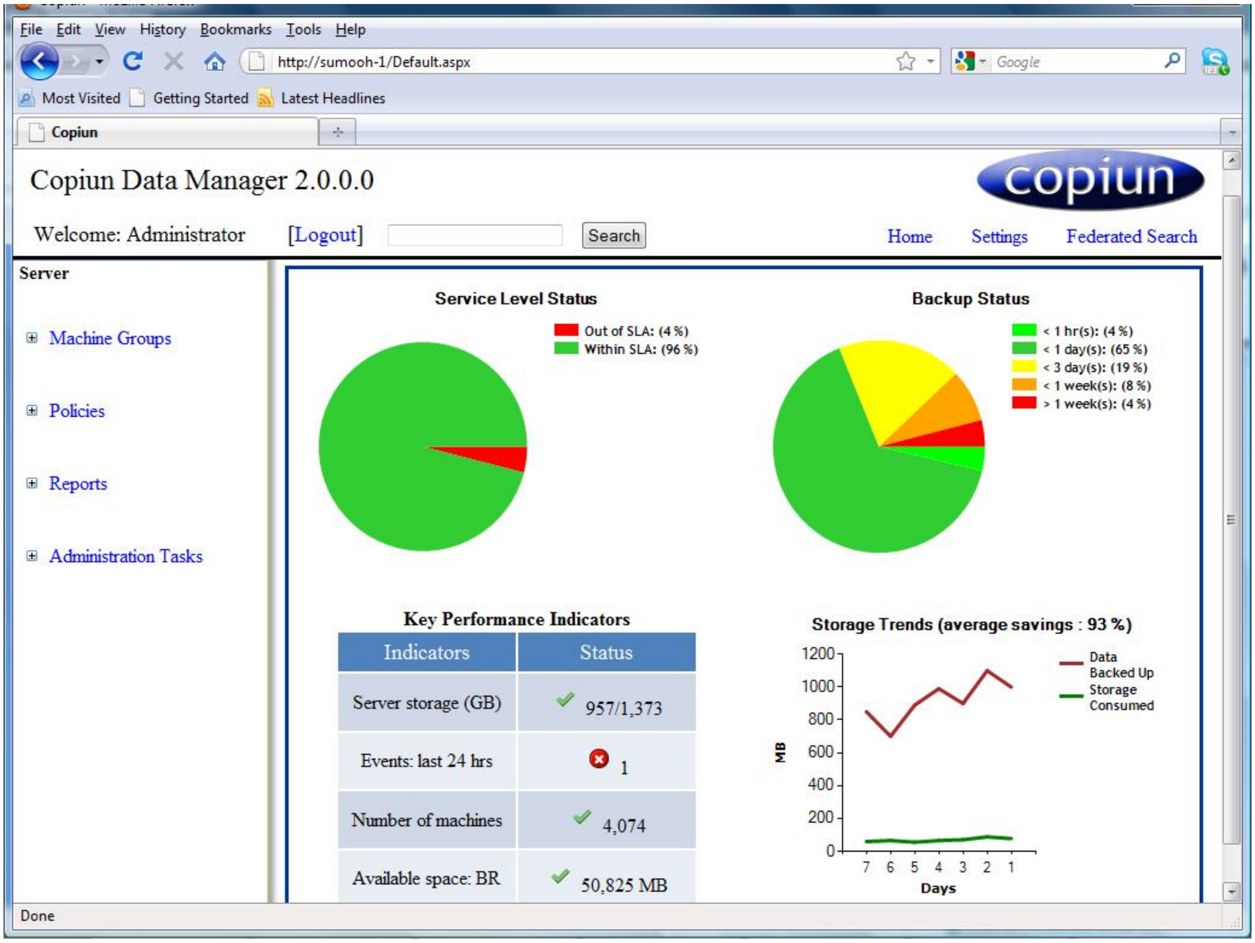
Copiun allows IT groups to create central policies which can then be applied to any number of PCs. The policies can be created for functional groups or sites. For example, you may want to define one policy for the Marketing group which backs up pictures and videos and another for the finance group which only backs up the “My Documents” folder. Click here to watch a video on how policies are created.

Machine Groups

Copiun allows IT to create machine groups which can mimic your current management units: i.e. functional groups or geographical locations or both. This allows you to manage the PCs and users in that group as an entity.

Service Level Based Management

Copiun is designed to make it easy for a single administrator to manage a large number of distributed PCs. On a day to day basis there are numerous false negative errors due to end user action, connectivity loss or PC shutdown. Copiun saves the administrators from having to worry about such false negative errors, by letting them define a service level, which is then automatically managed by Copiun Data Manager. As part of managing the service level it automatically detects and fixes most day-to-day environmental errors. The administrator receives a daily email and can also use the dashboard to quickly find out at-a-glance whether their machines are within the service level or not.



Key Performance Indicators

Indicators	Status
Server storage (GB)	✓ 957/1,373
Events: last 24 hrs	✗ 1
Number of machines	✓ 4,074
Available space: BR	✓ 50,825 MB

Ease of Deployment and Configuration

Server delivered as a virtual machine

CDM server is available as a fully-configured, ready-to-go virtual machine for both VMware and Microsoft Hyper-V environments, allowing you to setup the CDM server in a matter of minutes. Click here to download.

The CDM server is delivered in the .OVF format, therefore it can also be deployed in XEN Server environments.

Easy to deploy and update PC agent

CDM PC agent is delivered as a standard .MSI package, which can be deployed using Active Directory GPO or any other standard deployment tool in your organization.

Updates to the agent software are managed from the CDM Administration GUI, allowing you to selectively update a few PCs first before doing a mass upgrade.

No schedule management

Copiun Data Manager is a self balancing system, which doesn't require any schedule management on the part of the administrator. As new PCs enter the company or older PCs leave, CDM Server automatically ensures that various PCs are getting backed up at different times.

Centralized licensing

All licensing for PC agents is managed centrally, requiring no actions to be performed on the PC.

Security

Copiun Data Manager has been designed from the ground up to include state-of-the-art security measures to safeguard your corporate data. This section provides highlights of the key security measures.

Encryption

All data that is stored and transmitted over the wire by the CDM PC Agent and the CDM Server is encrypted using AES 128-bit encryption.

A unique pair of AES 128-bit keys is generated for every network session between the CDM Server and the CDM PC Agent – ensuring that the transmission is virtually unbreakable, because the lifespan of the keys is so short-lived. The keys are exchanged in a secure way using the public key of the CDM Server.

The symmetric keys used by the CDM Server for encrypting data for its data store are never shared with the CDM PC Agent, providing another layer of security.

Backup server always behind the firewall; No incoming ports need to be opened

Many other solutions require that their backup server be placed outside the firewall or incoming firewall ports be opened to enable remote users to connect without VPN. With Copiun, there is no need to place the CDM server outside the firewall or to open any incoming firewall ports. Through the Constant Access Gateway option mentioned earlier, remote users can be backed up in a completely secure way even if they are not connected via VPN.

Integrated into Active Directory

Copiun is fully integrated into Active Directory and provides single sign-on capabilities. There is no need for Administrators or end users to remember another set of credentials as everything is accessible using your existing Active Directory account.

Recovery audit logs

CDM Server logs every recovery operation performed on the CDM Server, whether from the CDM Server console or via the web browser. This helps maintain an audit trail which can be used to monitor any unauthorized data access activity.

Beyond Backup

In addition to providing an efficient and reliable backup and recovery solution, Copiun Data Manager provides several ways to leverage the backup repository for day-to-day operational use cases.

Federated search

Copiun Data Manager enables authorized users to perform a federated search across the entire PC data in the company to meet your organization's needs around E-Discovery and pre-emptive internal forensics. With this capability, servicing an E-Discovery request for PC data becomes straightforward as there is no need to go through the pain of physically getting a hold of PCs which may be geographically distributed. It also allows authorized users to search corporate data on PCs to detect potential risky behavior without requiring end user involvement. With Copiun Data Manager, you can perform a full search across the entire PC data regardless of the physical location of the PC and whether it is turned on or not.

Rapid risk assessment for stolen laptops

When a laptop gets lost or stolen, the first question on everyone's mind is: what was on it? Copiun Data Manager enables you to quickly create a searchable catalog of the stolen laptop's data – enabling you to rapidly assess any risk or exposure.

Access Anywhere

Copiun Data Manager enables IT organizations to allow their end users to access their PC data from anywhere using a Smartphone.

ADDITIONAL RESOURCES

Blog

a) Enterprise Desktop Laptop Backup Planning

Videos

b) Full-text search based self-service recovery

c) Configuring policies and PCs for backup

Downloads

d) Free evaluation version of Copiun Data Manager

Bibliography

Enterprise Strategy Group. *Data Protection Market Trends.*

Gartner. *Options for Enterprise PC Backup Still Limited (G00160375).*

Pepperdine University. (n.d.). Retrieved from http://gbr.pepperdine.edu/033/dataloss.html

Ponemon Institute. *Airport Insecurity: The Case of Missing & Lost Laptops.*

SearchDataBackup. (n.d.). Retrieved from http://searchdatabackup.techtarget.com/news/article/0,289142,sid187_gci1356227,00.html?track=NL-1059&ad=710462&asrc=EM_NLN_7872723&uid=1103597

Wikipedia. (n.d.). *Telecommuting.* Retrieved from http://en.wikipedia.org/wiki/Telecommuting