Cibecs

7 ENDPOINT DATA PROTECTION MUST-HAVES

ACHIEVE BEST-PRACTICE BUSINESS DATA SECURITY

A CIBECS WHITE PAPER

7 Must-Haves for Business Endpoint Data Protection

"Organizations are waking up to the fact that they have important data on endpoint devices that is ***not adequately protected, but should be***"

Gartner

Your business data is the lifeblood of your organisation. From confidential financial records and staff information to business-critical documents, emails, contracts and spreadsheets.

Data loss on a single user machine invariably leads to **massive consequences.** From user downtime and IT support costs to detrimental reputational damage and severe financial and legal Corporate Governance consequences. This coupled with the risk of your company data being accessed by unauthorised individuals, makes data protection one of the **most vital IT and business responsibilities.**

"In addition to civil and criminal sanctions of data loss & breaches, such breaches can ***impair customer confidence***, lead to a ***loss of revenue and market share*** and damage brand and shareholder values.

Risks associated with the security of client data needs to be given the same ***priority treatment*** as other risks the business manages."

Julie DiMauro, Thomson Reuters Regulatory Intelligence

Data Protection Delusions:

3 Ineffective Data Protection Methods Your IT Department May Be Mistakenly Using

When you analyse your data security, **you may assume that your data protection is up to scratch.** Before we look at the must-haves for effective and secure business data protection, we first need to address and debunk the most common misconceptions around protecting company laptop and desktop data.

Here are the **top 3 Common Data Protection Myths** that create the traps that many business IT Departments fall into.

1. Expecting Users to do Manual Endpoint Backups

Many organisations still employ outdated manual backup policies that require users to take initiative and **backup their own files** to the central server or a cloud sharing service.

The Assumption

Users will take responsibility for backing up and protecting their own business files, and this will save time for IT.

The Reality

Users almost never follow policy. They don't have the time, they forget, their backups are irregular and instead they backup personal files such as photos, music and movies.

The Result

- This poses a **massive organisational risk** as large amounts of confidential, valuable and sensitive business data **remains unprotected.**
- Significant amounts of **storage is wasted** on non-business data being stored, such as music and movies, as there is **no central control over backup policies.**
- Business data can be lost, and **accessed by unauthorised parties.**
- The IT Department is **not compliant to Corporate Governance Laws.**
- If sensitive data is lost or accessed, which is highly probable, the business faces **legal implications and financial penalties.**
- IT projects such as **data migration for OS Upgrades and PC refreshes are slow, expensive and can't be effectively reported on.**

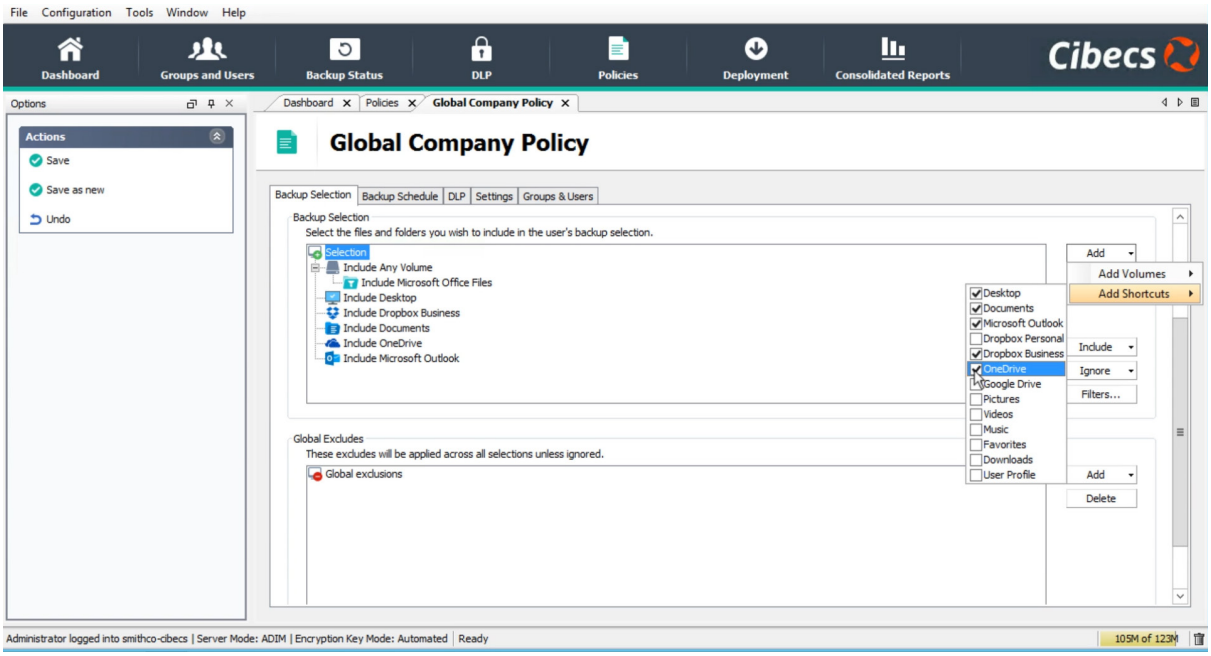
Data Protection Delusions:
2. "We've Got File Sharing, We've Got a Backup."

"Dropbox, Google Drive and Microsoft OneDrive are great for file-sharing – but they ***should never be used for business backups."***

James Kimbley – Founder of Google Cloud Partner Kimbley IT

With the proliferation of online file sharing services such as OneDrive and Dropbox, many companies have upgraded to a business account and are **using this as their 'Backup' system**. Often, y**our users have already turned to file sync and sharing** to provide the collaborative benefits they need.

They can access data from multiple devices and they can create and share content with others. However, this is **where the limitations of file sharing for data protection and data management purposes become clear.**



Data Protection Delusions:
2. “We’ve Got File Sharing, We’ve Got a Backup.”

The Assumption

Users are using it already so now we don’t need to manage, install and roll-out backups separately. **We can easily share, gain access to and recover files,** and it’s an easy and effective way to backup to the cloud for our company.

The Reality

These services are **not an endpoint backup replacement.** They do not provide the **data security and protection** of an effective user data backup product, and **if you are hit by Ransomware, that data can be infected**. You have **no central control** over what data is backed up, and **no reporting on data protection** across your business. **Any data users create outside these services is left at risk.**

File sync and sharing is great for file sharing and collaboration, but it **doesn’t provide the data security, management features and operational IT efficiencies** of a **purpose-built business** end user backup & protection system.

The Result

- Limited versioning results in lost files and is **not Compliant with Corporate Governance Regulations.**
- IT doesn’t have central control over data backups – and **company data is still at a significant risk.**
- The business **won’t be able to combat Ransomware Attacks,** and will instead be at risk of losing their files.
- If sensitive data is lost or accessed, which is highly probable, **the business faces legal implications and financial penalties.**
- The **data isn’t being compressed, deduplicated and managed efficiently** like with a leading backup system in place, the likelihood is a data explosion and unmanageable costs.
- **IT can’t pull reports** on data management projects, and has **no Audit Trail.**

Data Protection Delusions:
3. Choosing Backup That's Just Backup.

*"Endpoint backup is no longer a tactical product providing laptop file or device data recovery. IT leaders are looking for a **more strategic solution** to **centrally manage** user data that is typically unmanaged today."*

Gartner Research

The Assumption

Choosing a **bare-bones backup system** with **fewer features and add-ons is enough.**

The Reality

What your Business Management, Stakeholders and IT Department will get from a more **strategic backup system** with additional features, in terms of **operational and cost efficiency** as well as **Data Security and Compliance**, is of **utmost importance.**

The Result

The result will depend on the backup solution you implement. You can use our below checklist of Data Protection must-haves to evaluate potential acquisitions and compare endpoint backup solutions.

Get the User Data Backup Software Feature Checklist

7 Endpoint Data Protection Must-Haves

Endpoint data protection should be simple and easy to manage for IT. With the right tool-set and a well thought through strategy, protecting end user data can be **almost completely automated** and will allow you to **reduce operational costs and improve IT service delivery.**

The following **must-have software features** should be included in your chosen solution to ensure that you to overcome the most common obstacles in achieving **effective endpoint data protection:**

1. Simplified deployment & installation

While not being able to centrally manage and monitor your endpoint data protection is the single biggest obstacle to achieving success, **effective deployment and installation of the solution**, and future updates, is often one of the greatest technical challenges.

Must-have deployment and installation feature checklist:

- ☐ Easy, intuitive installation and wizard driven configuration
- ☐ Can be deployed to and installed on both **Windows and Mac** machines
- ☐ Option to **import user groups directly from Active Directory** (AD)
- ☐ Easily select which **backup policy should be used for different groups** or departments and edit default quota size
- ☐ Effective **built-in deployment** that allows IT to install the software easily and centrally to thousands of endpoints in a few hours
- ☐ Deploy easily across a **chosen IP range** or upload CSV with hostnames
- ☐ The solution should **automatically retry deployment if unsuccessful**, and IT should be able to **centrally control retry intervals** to ensure success
- ☐ Central, **real-time reporting** on deployment tasks
- ☐ **Easily scalable** across thousands of end user devices
- ☐ **User Agent package should be small** and IT should have the option of making the user agent **invisible to users**
- ☐ There should be **no impact on user machines** during installation to ensure success

In order to enforce the company's data backup and protection policy, **IT needs to have complete oversight and central control over the end-user data backup and protection environment.**

7 Endpoint Data Protection Must-Haves

2. Granular policy selection & control

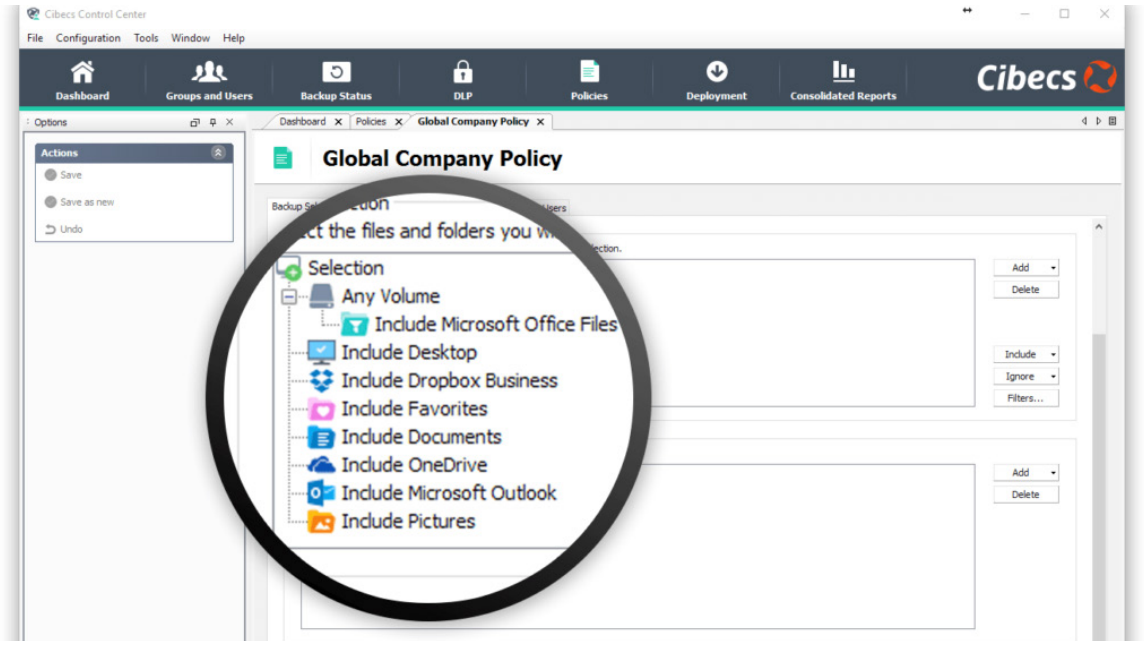
Must-have policy-setting checklist:

- ☐ **Central control** over data backup policies
- ☐ **Granular policy settings** per user, user group or department
- ☐ Ability to **easily select** file types or locations for backup
- ☐ Should include ability to **backup shortcuts** including Outlook and Desktop
- ☐ Additional policy management features such as setting user backup quotas
- ☐ Solution can backup and protect data stored in **Dropbox, OneDrive and Google Drive**

Central control should include the ability to **easily define data backup policies,** and should have **intuitive, granular selection options** that include backing up user common locations, file types and even their entire volumes – **minimising the risk of missing critical data** for backups because users store data in unknown and varied locations on their machines.

This means **increased control over what data is backed up** and **elimination of wasted bandwidth and storage** infrastructure. Different departments will have different requirements when it comes to selecting data for backups. As an example, your Marketing team may need videos, photographs and other media files to be backed up, where as your Finance department may not.

This complete, granular policy control given to an Administrator means **increased data endpoint protection and reduced unnecessary overheads.**



7 Endpoint Data Protection Must-Haves

3. Lightning fast backups with huge data and storage savings

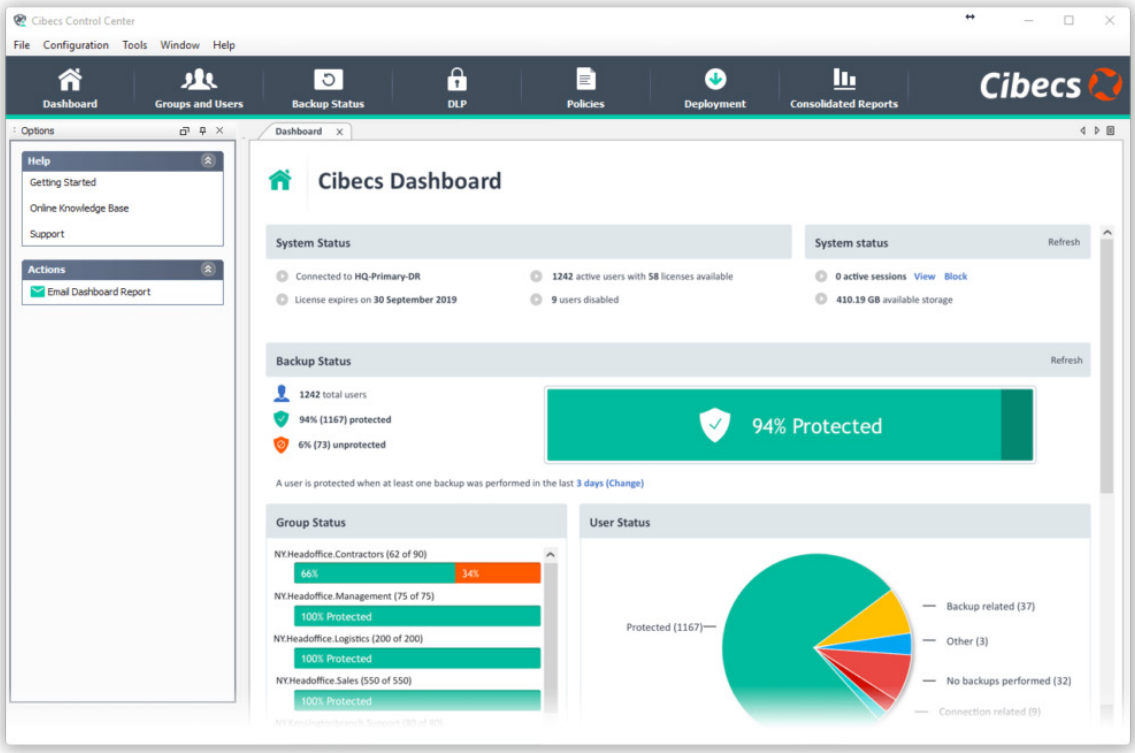
Must-have features:

- ☐ Complete **control over what data is stored** on the server
- ☐ Data **deduplication**
- ☐ **Only block level changes** of files should be backed up after the initial backup
- ☐ Central control over user **quotas**

Data should be **compressed before backup, de-duplicated** to drastically reduce storage requirements, and **only the block-level changes of files backed up on a daily basis.** This means better performance, effective use of company infrastructure and reduced impact on your network.

To further minimise the size of data that is transferred and stored, your chosen end user backup solution should **allow the administrators to centrally define a data selection policy** by department or user group. Setting these policies will ensure that **only business-related data is backed up**, decreasing the storage requirement and preventing unnecessary costs.

Effective management of data backups with central control over policies means huge savings on infrastructure costs.



7 Endpoint Data Protection Must-Haves

4. Simplified, secure data recovery

Must-have data recovery checklist:

- ☐ **Automated** daily user backups to ensure data is available for recovery
- ☐ **Opportunisitic backups** that automatically reschedule the backup task to ensure that your mobile workforce is effectively protected
- ☐ Fast, **wizard-driven data recovery**
- ☐ No unauthorised data restores
- ☐ Seamless **cross platform restores**
- ☐ IT can enable **users to recover their own files** when necessary
- ☐ **Simplified device refresh** and **Operating System migration**
- ☐ Ability to **revoke user access to files** and ensure that only authorised users restore data

An effective data backup and protection solution should allow for **fast, wizard-driven data restores** to ensure that data is easily recoverable in the event of loss. Data recovery should be a **simple process reducing user downtime and IT resource requirements.**

The solution must ensure that all user **files are safeguarded from unauthorised access** during the data recovery process, and that **only an authorised IT Administrator or user with a specific key can recover files.**

IT should also have additional data recovery security features for Data Loss Prevention including the ability to revoke user access to files, and remotely wipe all files from a user machine.

The ability to **quickly and easily recover and migrate user data** to a new machine or operating system gives your business the added benefit of **simplifying and accelerating data migration and hardware refresh projects.** This will provide your organisation with significant IT cost reductions as well as improved IT service delivery.

The benefits of an effective end user data backup & recovery solution during hardware refresh projects and OS migration:

- **Shorter user downtime and faster IT support** turnaround time as backed up user data can simply be recovered to the new device without manual intervention.
- **Eliminate the risks of data loss** as backed up data is not deleted or overwritten once recovered.
- **Prevent losing critical emails** and ensure Corporate Governance Compliance with Microsoft Outlook restore support, **intuitive reporting and the ability to track data restores.**
- **Overall improved efficiency** and reduced associated overhead costs.

7 Endpoint Data Protection Must-Haves

5. Complete Data Loss Prevention

Must-have included data loss prevention features:

- ☐ Automated and **centrally controlled** end user backups
- ☐ **Integrated endpoint file encryption**
- ☐ Ability to **remotely wipe data** from a user machine
- ☐ **Device geo-locate**
- ☐ **Data theft prevention**

Your chosen endpoint data protection solution, should equip your organisation with **powerful multi-layered protection** against any and all data loss, data corruption and unauthorised data access by offering **more than just endpoint backup.**

Look for a solution that includes **integrated endpoint encryption, remote wipe, and data theft prevention**. This means increased data security, lower economic impact from lost or stolen endpoints and complete Corporate Governance Compliance.

Endpoint File Encryption

Integrated endpoint file encryption provides increased data security as **files on the user device are automatically encrypted at the source** and are inaccessible to unauthorised parties if the device is lost or stolen.

Remote Wipe

Remote Wipe enables your administrator to **remotely delete user data** quickly & easily, directly **from the Control Centre**. This means IT has **complete control over any access to company data should a user laptop be lost or stolen.**

Device Geo-Locate

Should a laptop be lost or stolen, IT can enable remote geo-location of the device, pinpointing the **exact location of that machine as soon as it goes online.**

Data Theft Prevention (DTP)

Data Theft Prevention enables organisations to **automatically revoke user access to data after a set timeframe.** IT can centrally set the timeframe within which user computers should have connected to the server, for example 30 days.

If a user's computer hasn't connected to the network for this defined period of time, access to data is automatically revoked. This is an incredibly powerful fail-safe that IT can put in place to ensure the **highest levels of data security.**

This automated, time-based DTP creates an important **added layer of protection against data theft across large organisations** where it is more difficult for IT to manually monitor all machines.

7 Endpoint Data Protection Must-Haves

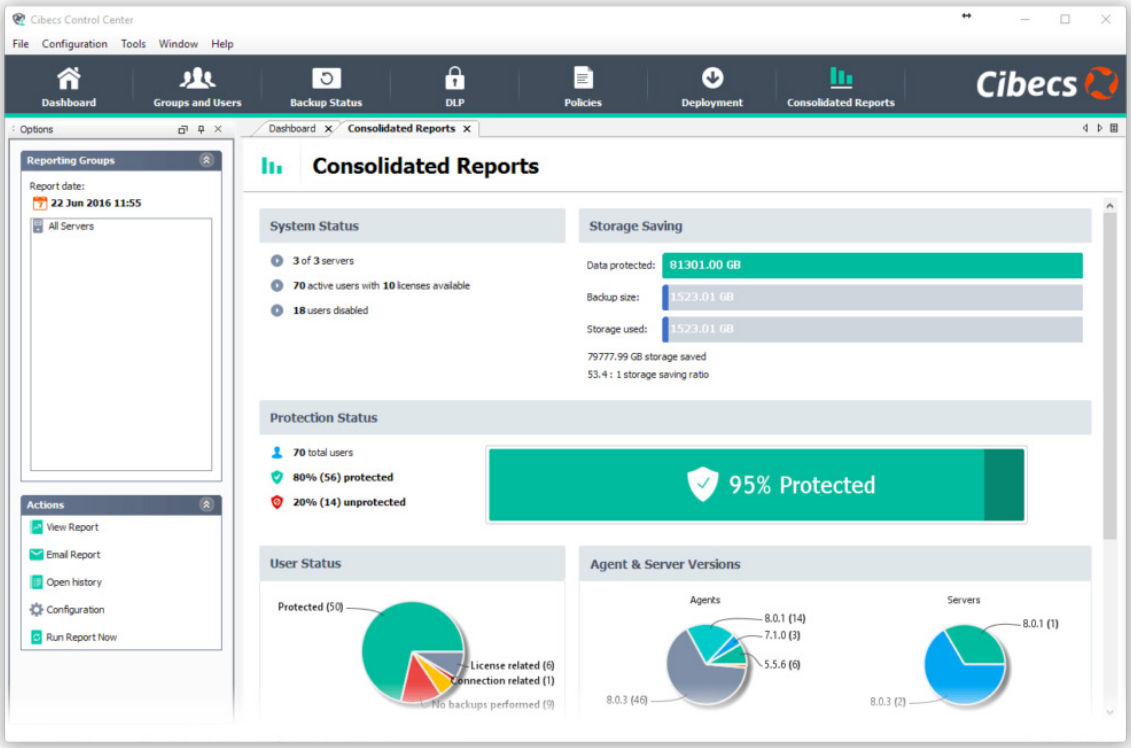
6. Central reporting with consolidated metrics

Must-have reporting features:

- ☐ **Reporting dashboard** with real-time metrics
- ☐ Single **consolidated data protection** metric for your entire business
- ☐ Scheduled **email** business reports and actionable technical reports
- ☐ Ability to monitor any data loss risks and address them
- ☐ **Consolidated reporting** across multiple branches or servers
- ☐ Ability to **track and report on data restores**

When selecting a solution, it's imperative that it provides IT with **simplified, real-time metrics** for reporting on your data backups and data protection. You should be able to monitor your entire company's data protection from a **single consolidated metric**, and narrow down to specific user groups and users to **isolate any data loss risks and be able to address them.**

The management and reporting interface should be **intuitive and easy to use,** with powerful reporting and management features. You should be able to receive **reports specifically designed for business management** with metrics valuable to business stakeholders, as well as **actionable technical reports** based on technical data required to **make managing data protection easy for IT.**



7 Endpoint Data Protection Must-Haves

7. Corporate Governance Compliance

Must-have data protection features:

- ☐ Ability to **define and implement a data backup and data protection policy**
- ☐ Ability to **demonstrate proactive data protection** management and compliance
- ☐ User friendly **reporting with both technical as well as business metrics**
- ☐ Ability to report on and pull an **Audit Trail of data restores**

Data loss prevention for complete data security and Corporate Governance Compliance

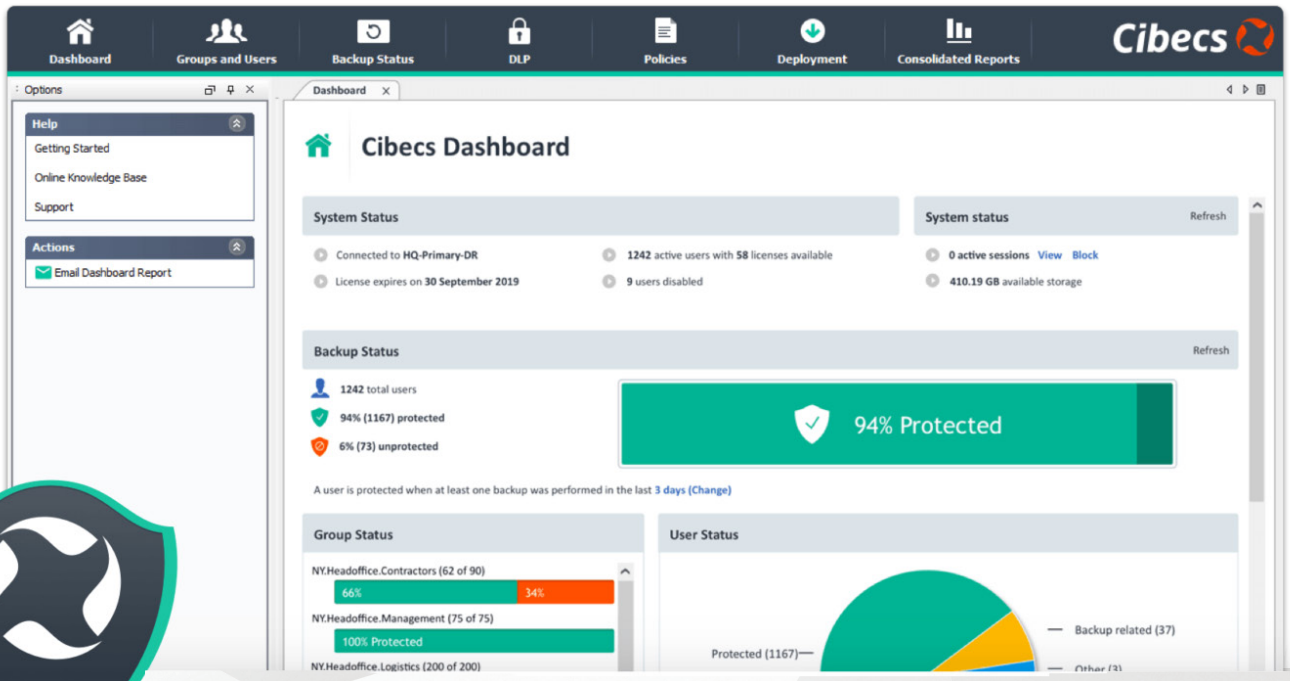
It has become a business **imperative to protect sensitive company, customer and staff data** from theft and unauthorised access, and for companies to be able to **prove that they have a well-defined data protection strategy in place.**

Businesses face f**inancial penalties, legal consequences and huge reputational damage** should they fail to implement the correct data protection strategies and solutions, and be able to monitor and report on it.

While the ability to backup and recover data is an important foundation to compliant data protection, and ensures that you are able to continue business uninterrupted, **data loss prevention increases your data security** and provides your business with **complete protection against the loss of and access to business files.**

"Cibecs intuitive reporting allows for reports based on user activity. You can see whose data has been backed up, how protected your users' data is and pull management reports to prove legal compliance and adherence to good corporate governance."

Cathy Harris – IT Manager, Clinix Health Group



About Cibecs

Cibecs is the best backup & data protection for business. Cibecs is built for complete endpoint data backup and protection that ensures the security of data stored on endpoint devices, as well as valuable and operational data management benefits.

Some of the Cibecs features

- **Backup & Recovery:** Automate and centrally manage the secure backup & recovery of endpoint data.
- **Local Data Encryption:** Powerful, endpoint file encryption means your files are always secure.
- **Device Geolocation:** Quickly & easily locate lost or stolen devices.
- **Remote Wipe & Data Theft Prevention:** Remotely wipe data or automatically revoke access to data.
- **Corporate Governance Compliance:** Powerful security features and intuitive reporting enables compliance to Corporate Governance legislation
- **Device Refresh & Migration:** Faster & simpler PC refresh projects and OS upgrades

Cibecs encompasses all these critical end user data protection elements in a single solution that is not only cost-effective but can be deployed, managed and monitored from a central dashboard.

Cibecs is trusted and used internationally by companies and government agencies in North America, Europe, South Africa, Africa, Asia and Australia. To view a full demonstration of Cibecs click here.

Get in touch with Cibecs

Facebook www.facebook.com/cibecs
Twitter @Cibecs
LinkedIn www.linkedin.com/company/cibecs
info@cibecs.com
www.cibecs.com

Fortuna Data
01256 331614
sales@fortunadata.com
www.fortunadata.com
www.data-storage.uk
Providing IT Solutions for Businesses
Founded 1994 based in Basingstoke, Hampshire

Cibecs is Used & Trusted By

BARCLAYS SAMSUNG INGRAM MICRO CNBC