A Technical Evaluation Framework for Selecting an Endpoint Data Protection Product

Written by Cibecs - https://cibecs.com/endpoint-backup-security-quiz/

Objective: *This framework is intended to demonstrate a holistic view of the essential endpoint data security features every company needs to ensure a safe and protected endpoint data environment. This framework includes a detailed breakdown of key considerations, a product, operations and business evaluation table and an essential endpoint product requirements checklist.*

In order to never lose end user data again and safeguard against ransomware with minimal resources, you are going to need the right set of tools to get the job done. There are a few essential features you cannot be without when it comes to your endpoint software, or the combination of tools required to automate tasks and gain visibility and control over your organization's environment.

In this informative guide we will provide you with all the details you need to select the best endpoint security system.

In the multi-faceted landscape in which today's organizations operate it is essential to take a multi-layered pre-emptive approach towards endpoint data backup, protection, management and security through utilizing the right set of tools or a comprehensive product that covers all the essentials.

More importantly the selected solution needs to optimally utilize company resources, such as bandwidth and storage, and be able to run without impacting users' productivity.

Ideally, you should select a product that can cover all your data backup, security and protection needs as this will provide a simple solution reducing the chances for error and ensure complete protection. The alternative would be to use multiple tools which can be confusing, need to be managed and may be problematic if tools aren't compatible with one another.

When examining which product/ products to select to ensure endpoint backup, security and protection there are three main areas to consider:

Area	Considerations
Product Features	• What features are covered? • How comprehensive is the system? • Do the features and capabilities meet IT's functional and technical needs?
Operational Considerations	• How well can the product integrate into the organization's environment? • How is the software deployed? • How will the product impact the network, users, bandwidth and other company resources? • Is the system easy to manage? • Can it be implemented in a complex environment with both local and remote endpoints?
Business Criteria	• Cost versus terms of coverage? • How scalable is the product and can it work for a dynamic organization? • How intuitive is the software to use? • Is the system compliant and can it assist with corporate governance needs? • Does the product have reporting capabilities? • How is the product licensed? • Does the software provider have a support structure & provide training?

Essential Endpoint Product Features & Capabilities		
Feature	**Required Capabilities**	**Benefit/ Outcome**
Discovery & Inventory	Discover devices on the network to create visibility.	You cannot protect, backup or secure devices you do not know you have. It is imperative that the solution you select can find all your organization's endpoint devices and create an accurate inventory of all hardware, software, and data regardless of where it is stored. This provides the ability to gauge the amount of storage required for protection.
	Detailed inventory of business data by file type & location to understand risk.	
	View detailed hardware & software inventory for each device, including installed applications, drivers, services & updates.	
Backup & Recovery	Define a detailed policy of what data should be protected.	A comprehensive data protection policy that covers all the critical company data based on facts ensures essential data is backed up & nothing slips through the cracks.
	Set granular policy details for groups of users or departments.	Guarantees the right data is protected, and company resources aren't wasted.
	Automate the deployment, implementation and monitoring of the policy.	By using a product that automates deployment, implementation, and monitoring, ensures policy is being followed as there is zero chance of users not following policy.
	Automate CDP user backups to a secure central store preferably using source-based deduplication.	Snapshots allow for point in time recovery. Accessing data from your archive is simple and fast, as independent snapshots mean that files from any point in time can be accessed instantly.

		Archival of backed up data is crucial as it is a way to protect against ransomware, data corruption and user error. Data should be backed up in a continuous manner to reduce these risks. Optimally utilizes company's bandwidth & storage, ensures complete automation of the backup tasks that cater for connectivity, compression, security and locked files. Utilizing source-based deduplication to eliminate redundant data from the client before it is stored, improving overall performance & reducing data storage expenses.
	Authorized users can recover their own data through single click recovery.	By having this capability in place, users can simply recover files or find a deleted document without IT. Freeing up IT resources which can be allocated elsewhere.
	All backup & restore events are monitored & recorded.	All backup and restore events are tracked and various filters are available to ensure policy compliance.
Central Cloud Management & Reporting	User Agents can be centrally activated after the discovery agent has been deployed.	The selected endpoint product needs to have a central cloud management system from which IT managers can view and control the organization’s endpoint environment, regardless of users’ locations. In other words, the endpoint solution needs to provide IT with the ability to implement certain actions on end user devices remotely. This ensures a device can be secured even if it has been lost or stolen and the valuable data can be encrypted, wiped or endpoint located, no matter where or with whom the device is.
	All discovered devices, device protection, team policies and vaults are managed from one cloud management console.	
	Protection policies are centrally configured and enforced to ensure compliance.	
	Capture protection status for each device in the environment & communicate it to the cloud console.	Endpoint data is sent to the cloud to provide a complete contextual picture for real-time data backup, security & protection.

	Provide a single protection rating across the environment to measure protection.	A single protection/ security metric makes it easy to monitor the organization's level of protection no matter the size or complexity of the environment.
	Set criteria & establish report metrics for automated customised reports.	Provides IT with the ability to report on all hardware, software and data across the organization through automated reporting capabilities that require minimal time investment.
	Automate report creation & distribution to key stakeholders through email.	The reporting system should provide predefined reports that can be used and emailed to different departments or groups and allows for automated email reporting.
	Centrally managed security & DLP	Centralized management gives IT full control over Data Security, while being able to action threats from one centralized point regardless of the size of the organisation and where users are located.
File-based encryption	File-based encryption is set at policy level to ensure the right data is encrypted.	Global compliance legislation requires all company data to be encrypted. By using a product that allows encryption to be set at policy level and implementation automated, the compliance to data protection laws no longer needs to be a headache.
	Automate encryption key management.	Having the ability to automate encryption key management prevents user error, the inability to recover keys & frees up IT resources that would normally be used to create, implement & manage these encryption keys.
Remote wipe	Automate the deletion of unwanted data or data at risk of unauthorized access through forensic level deletion capability that can be centrally managed.	Utilizing a tool or product that can wipe a user's device on a forensic level is essential to prevent data from falling into the wrong hands or unauthorized access being gained to sensitive company data.
Remote device access management	Remotely revoke user access to data in the event of device loss or theft, or if a user leaves the organization.	Through utilising a product that provides central device access management it is easy to remotely revoke access to ensure data is always protected.

	Enable auto revoke through a timer to automatically encrypt, wipe or revoke access to devices that have not made contact to the network in some time.	Auto revoke is also a great tool to pre-empt data vulnerabilities and ensure valuable user data is always protected.
Device Geo-Location	Enable Geo-Locate on activated devices to quickly identify their whereabouts if lost or stolen.	When a device is lost or stolen, IT can track the location of any protected device for quick recovery or remote wipe, increasing the chances of recovering your device and the confidential data on it.
Full remote migration	Remotely trigger and monitor device migration.	Streamline the process of migrating a user to a new device by minimizing the resource time needed to move the data. The user should be able to continue with their work while the migration process runs in the background, ensuring the least amount of user down time while performing this task.
	Full device-to-device migration that ensures user files are restored to the original location.	
	Live Migrations	

Operational Considerations		
Requirement	**Consideration**	**Evaluation**
Endpoint platform coverage & compatibility	Does the selected service provider support the current endpoint environment size?	Review whether there will be any product-related performance limitations for the number of endpoints in the organization.
Provide a simple to use central cloud-based management system	Is the product's system easy to use & does it provide IT with complete visibility & control regardless of locations?	Evaluate overall platform to identify overall ease of use, simplicity of navigation, features access as well as support or help features. The benefit of a secure cloud management system is that it requires no on-premises support & software updates are automated.

Endpoint deployment	How is the software Agent deployed? Is deployment & implementation automated or is it a manual process?	Evaluate the ease of endpoint management through the chosen product. Consider the simplicity or efficiency of deployment, configuration & maintenance as well as the impact on IT resources.
Configuration & updates	Does the product provide a variety of ways to configure & update endpoints? Does the software provide automated central administration as well as local administration so users can action minor tasks themselves?	Evaluate the — impact of the endpoint updates on users — the effectiveness of cloud-based deployment — the product's ability to implement policies automatically across all endpoints
Endpoint communication with the cloud	Does the selected product provide bidirectional communication between endpoints and the cloud management system to ensure comprehensive & complete monitoring of the environment?	Be sure to understand the resource requirements needed to maintain the real-time communication between endpoints and the cloud such as: — Bandwidth - Latency — Uptime - Redundancy
Endpoint user impact	How does the Agent/ software impact endpoint memory (RAM)? How does it impact the storage capacity of end user devices to seamlessly integrate & automate tasks?	Identify how the product will impact users. Ideally, a product that is lightweight & has little to no impact on the endpoint system & requires little resources is best.
Status monitoring from a central management console	Does the selected product have the capabilities to support ongoing automated monitoring of endpoints, such as? - a simple intuitive dashboard to communicate overall status of endpoints across the organization, - a more granular detailed status for each user device.	Evaluate monitoring capabilities and how accurate information provided through the consolidated central cloud dashboard is.

Business Criteria / Considerations		
Requirement	**Consideration**	**Evaluation**
Scalability & growth	Can the product scale to accommodate a dynamic or growing organization?	Determine whether the product will scale to meet growth projections without issue.
Deployment model	What type of deployment does the vendor make use of? Is the deployment delivered through a manual process, the cloud or is an alternative method used?	Evaluate the costs versus the benefits of the type of deployment provided by the selected vendor. This process will determine which model best supports the Organization's endpoint environment & technical requirements. Be sure to confirm how long deployment will take and whether the process will disrupt users or productivity in any way. Ideally, selecting a cloud deployment method that utilizes a single unified lightweight agent reduces complexities and processes, simplifies management, and ultimately decreases the total cost of ownership (TCO).
Compliance validation & verification	Can the selected vendor verify their processes are in line with data protection requirements? How does the product ensure certain compliance criterion is being met and through which features? Is the product able to support the needs of the business relative to compliance mandates & requirements?	Ensure that the product itself is SOC 2 compliant & that it can provide IT with the evidence needed to showcase compliance to data protection laws.
Licensing	How is the product licensed? What is included in the license & are there any limitations?	This information can be used to determine the total cost of ownership (TCO) & will take into consideration: - initial setup time - hardware costs, - deployment time, - cost of resources required for ongoing management
Support structure	What type of support structure does the vendor make use of for example: - is support provided during specific hours only? - is support available 24/7?	Support is essential to ensuring problems can be corrected as soon as possible. Below are essential questions to ask your selected provider: 1. What are the different support options available & how do they work?

	- does it support availability or does it depend on the package selected?	2. Is local support available or provided through partners? 3. Is it possible to speak to a real person if necessary?
Product training	Does the vendor provide ongoing or once-off training? Is training made available through a variety of formats? Are courses tailored to different stakeholders i.e., IT administrators versus users?	Is the training provided sufficient & does it meet the various organizational needs?
Service Level Agreements (SLAs)	Beyond the SLA agreement between the vendor and the organization. Does the product provide a simple unified SLA metric IT can use to communicate the level of the organization's endpoint protection that can easily be communicated to stakeholders through automated reports?	A single SLA rating to showcase protection empowers IT & provides an easy way to emphasize protection. In addition, it is essential that you evaluate the SLA agreement between the organization and the vendor & that it at least covers the following areas: - Security & privacy - Redundancy - Bandwidth - Response time - Disaster recovery - Non- performance - Access to an online data backup facility - Compliance validation
Vendor stability & growth path	How long has the business been in existence? Do they have a broad customer base? Have they been able to adapt to the fast-paced industry to continually stay at the forefront on the endpoint backup, protection & security?	Don't be afraid to ask providers for client reference lists, case studies or whitepapers that showcase their expertise & how their solution can integrate with different businesses. This is a great way to determine if the vendor you have identified will be the right fit for you & your organization. Determine whether the vendor's growth path for the product aligns with your organizational needs. It is essential that you partner with a vendor that believes in continuous improvement to stay ahead of the game & provide you with an ongoing high-level solution.

Conclusion

The best way to ensure that you select the right endpoint data protection product is to completely understand your organization's product, operational and business requirements. Armed with this information you can create an evaluation matrix that can be used to analyse the solutions available based on the organization's requirements.

Additionally, it is essential to think long term when selecting a vendor to partner with as endpoint data backup, security and protection is likely to become more complex as a result of the fast-adapting technological environment. You need a partner that can go the distance and operates with the end user in mind.

Endpoint Backup, Security & Protection Product Requirements Checklist

No.	Specification	COMPLIANCE		Reference / Comments
		Comply	Not Comply	
	1. Compulsory Business Requirements			
1.1	The organization requires the implementation of the product to be done by a Certified Service Professional – vendor certifications to be attached.			
1.2	The requirements outlined in the Terms of Reference must be met as part of an integrated solution configurable through a single, unified management console.			

1.3	In accordance with compliance and regulations with regards to data security and access, the software solution and the vendor should have a zero-knowledge encryption key management system.			
1.4	Customer references must be available upon request.			

No.	Specification	Compliance Comply	Does Not Comply	Reference / Comment
CRITICAL REQUIREMENTS				
1.1	**Single Data Backup & Protection Solution** The solution must include: a. Integrated Device & Data Discovery & Inventory b. Endpoint Backup & Recovery c. Local Data Encryption d. Remote Wipe capabilities e. Remote Revoke of access to data f. Device Geolocation g. Integrated full device to device migration of all data, profile and settings.			

	All of the above must be available as part of an integrated solution configurable through a single, unified management console.			
1.2	**Integrated Discovery, Inventory & Deployment** The system must include integrated discovery and inventory of user devices (including data, hardware and software) & agent deployment to streamline the rollout process and ensure full implementation of the solution. The above must be available as part of an integrated solution configurable through a single, unified management console.			
1.3	**Hybrid Cloud** The system must be available as a Hybrid Cloud solution. a. The solution must provide a centrally hosted Cloud application that enables control over all aspects of configuration, management & monitoring. b. The system must allow for the storage servers, where backed up data is stored, to be located on premise securely behind the firewall at the head office or branch offices.			
CENTRAL CONTROL & MANAGEMENT				
CENTRAL MANAGEMENT				

1.4	The system must allow for complete central management and monitoring across multiple sites and storage servers from a central console within a single unified view without having to manage sites separately.			
BACKUP POLICIES				
1.5	The system must allow for extensive central control over all aspects of user backups.			
1.6	**Centrally set & configure backup policies to ensure inclusion of business-critical data and exclusion of non-business data** a. Backup filters must be able to include files based on file extensions independent of where the data is stored, for example: Office Files located everywhere on the device b. Backup locations should be configurable to include data in specific locations such as My Documents, Desktop, etc. c. Backup filters must be able to excludes files based on file types and path to ensure that non-business data is not included. d. Backup filters must also cater for Microsoft Outlook Archive (PST) Files regardless of where they are stored.			
1.7	**Backup scheduling** a. The system must allow for Near Continuous Data Protection scheduling with backups occurring on an hour-based frequency. b. The system must allow for a scheduling option that will consider the user's computer not being powered on or			

	connected to the network at the time of backup and reschedule backups accordingly.			
1.8	**Backup policies for different groups** a. Policies must be defined centrally and must automatically be applied to the users without the need for manual configuration on a per user basis. b. The system must allow for policies to be defined per group of users.			
DEVICE DISCOVERY, INVENTORY & REMOTE DEPLOYMENT				
1.9	**Device Discovery & Inventory** a. The system must allow for all endpoint computers on the network to be discovered automatically. This is to provide the organization with a full inventory of all user computers that are at risk and that should be protected.			
1.10	**Data Discovery** a. The system must have the ability to discover all data located on user devices. b. The system must be able to classify discovered data into business and non-business data to highlight the amount of data that is at risk and the amount of storage required to protect it.			
1.11	**Hardware & Software Inventory**			

	a. The system must provide a detailed list of computer hardware for each device to assist in hardware refresh planning. b. The system must also provide a detailed list of installed software including applications, drivers, services & updates for each user's computer to aid recovering the user to the same configuration.			
1.12	**Integrated Remote Deployment** a. The system must allow for the data protection client software to be remotely and silently deployed without requiring any user intervention. This must be done from within the application and must not require any external processes.			
1.13	**Active Directory Cloud Connector** a. Given that the system must provide for centralized Cloud management, it must also allow for on-premise Active Directory users to be authenticated during the client application installation through the means of a connector that can be installed on-premise. This is to allow users of the system to be authenticated and identified without requiring user credentials to be entered.			
1.14	**Automatically protect new devices** a. The system must be able to automatically discover new user devices on the network and provide the ability to automatically protect them.			
1.15	**Automatically classify inactive devices**			

	a. The system must be able to automatically classify devices as inactive for user's that have left the organization. This is to reduce the management overhead of having to manually manage this process and to ensure accurate management and reporting.			
ENDPOINT BACKUP & RECOVERY				
BACKUP				
1.16	**Automated backups** a. Backups must occur automatically without requiring the user to initiate the process and without any user involvement.			
1.17	**Activity based performance throttling** a. The client application must be able to detect if the user's computer is in use and throttling the backup process to ensure no impact to the user. The client application must also be able to detect if the computer is idle and reduce throttling to allow backups to complete faster.			
1.18	**Backup open files** a. The system must provide integration with Microsoft VSS (Microsoft Volume Shadow Copy services) as it must allow users to continue to work on open files while the backup runs in the background.			

1.19	**Secure transmission of backup data** a. Backup data must be securely transmitted to the backup server using SSL.			
1.20	**Optimization for backing up Microsoft Outlook Archive Files (PSTs)** a. The client software must be able to efficiently detect changes in Outlook Archive PST Files to reduce the backup time.			
1.21	**Large file support** a. The client software must support a mechanism for quickly processing changes in large files such as PSTs.			
1.22	**Global Source & Target Based Deduplication** a. The system must support Source Based Deduplication technology to ensure any parts of user data that is already stored by any other user is not transferred again. This is to reduce unnecessary network usage. b. The system must support Global Target Based deduplication technology and only store duplicated data shared amongst all users on the system once to reduce storage requirements.			
1.23	**Support for Roaming & Mobile workforce** The system must provide for mobile users backing up over an internet connection with limited speed and bandwidth availability.			

RECOVERY				
1.24	**Granular data restores** a. The client software must provide the ability to restore all or specific files.			
1.25	**Users must be able to restore files** a. Self-service recovery must allow users to restore files.			
1.26	**Data Migration** a. Recovering data to a different version of the operating system where it was backed up, must migrate all of the common locations such as Desktop and My Documents to the new version of Windows to allow for migration scenarios.			
1.27	**Profile Settings Restore** a. The system must support restoring the user's computer profile include system and application settings.			
DATA LOSS PREVENTION				
LOCAL DATA ENCRYPTION				

1.28	**Centrally enable encryption** a. The system must allow for local data encryption to be centrally enabled on all user devices without any user intervention and must encrypt all of the user's files on their local computer as centrally defined.			
1.29	**Transparent encryption & decryption** a. Both encryption and decryption must be completely transparent to the user as to not interfere with the users work.			
1.30	**Industry standard encryption** a. The encryption must be secure and must leverage industry standards.			
1.31	System files must be excluded from the encryption process to eliminate unnecessary impact on end users caused by whole disk encryption.			
REMOTE WIPE				
1.32	**Centrally manageable** a. The administrator must be able to request all selected data to be deleted from the local device.			
1.33	**Secure delete** a. The deletion of data must be secure to ensure that it cannot be recovered using data recovery tools.			

1.34	a. The administrator must be able to check whether a remote wipe request has been successful.			
REVOKING OF ACCESS				
1.35	**Revoking access** a. The system must allow for access to user files located on their local device to be remotely revoked on demand.			
1.36	**Automatically revoke access** a. The system must allow for access to user files located on their local device to be revoked if the user has not connected to the network for a defined period of time. b. The revoking of access must not be destructive and must be reversible.			
1.37	**Remotely grant access** **a.** The system must have the ability to remotely grant access to the user's files if access was revoked.			
DEVICE GEOLOCATION				

1.38	**Central device geolocation** a. The administrator must be able to centrally request the location of a device. b. The location must be displayed on a map with a street address.			
FULL REMOTE MIGRATION				
1.39	**Remotely trigger and monitor device migration** a. Migrations must be triggered from the management console b. The migration process must be remotely performed without needing to have physical access to the user's computer. c. The administrator must be able to see the status and progress of a migration. d. The administrator must be able to trigger and monitor multiple migrations simultaneously.			
1.40	**Fully automated** a. The migration must be fully automated and without requiring a whole set of configurations or setup.			
1.41	**Full direct device migration** b. The migration must be directly performed between the old and new device over the network to eliminate any additional storage requirements.			

	c. The migration process must be able to detect the fastest network route in the event that the user has both ethernet and WIFI connectivity. d. The migration process must compress that network transfer. e. The communication between the old and new device must be encrypted. f. The migration process must have network retry-ability. g. The migration process must be able to automatically open and again close the firewall ports for the user's computer.			
1.42	**Background migration** a. The migration process must be able to run while the user continues to work. b. The migration process must be able to do a subsequent update migration without migrating all of the files again and only migrate any new or changed files so that the person can be rerun if need be.			
1.43	**Migrate all files and settings** a. All files on the user's computer including business and personal files must be migrated. b. The migration process must skip system and application files to avoid causing any corruption to the new computer's configuration. c. The migration process must place files in shortcut locations such as Desktop and Documents in the correct new path on the target device even if their paths have changed.			

	d. The user's profile settings including task bar settings, folder options, network drives, Outlook and all associated configurations must be migrated.			
PROTECTION COMPLIANCE & REPORTING				
1.44	a. The system must provide a single metric to identify the percentage of computers that are protected against data loss and meet compliance requirements.			
1.45	a. Filtering must be available to allow for the protection metric to be monitored per department or groups.			
1.46	a. The system must be able to classify users and devices into categories of risk versus protected to simplify reporting across thousands of devices and must consider a protection window for classifying the user so that user's that have backed up in the last x days can still be considered protected rather than seen as an incorrect risk.			
1.47	**Reporting API** a. The system must provide for a reporting API to allow for both custom reports as well as integration with existing systems.			
SECURITY				

1.48	**The system must provide snapshots of backed up files.** a. The system must have the ability to restore from previous point in time snapshots.			
1.49	**Strong Data encryption on backed-up data.** a. The system must encrypt the backup data at rest using AES 256-bit encryption and			
1.50	**Zero Knowledge Encryption** a. The system must provide for zero knowledge encryption to ensure that the encryption keys are never exchanged with the storage system at any point in time.			
1.51	**Zero Knowledge Encryption Key Management** b. The system must implement a mechanism for managing encryption keys that is seamless and does not require Administrators to enter encryption keys for users that are authenticated by Active Directory.			
SUPPORTED PLATFORMS				
1.52	The client application must support all currently supported versions of Windows.			
1.53	The server software must support operating on Windows as well as Linux.			

No.	Specification	COMPLIANCE		Reference / Comments
		Comply	Not Comply	
2. Implementation and Support				
2.1	Detailed project plan outlining proposed implementation, support and services to be attached			

No.	Specification	COMPLIANCE		Reference / Comments
		Comply	Not Comply	
3. Location of sites				
3.1				
3.2				

3.3				
3.4				

Competitor Matrix

	Cibecs Endpoint Cloud	Symantec / Veritas DLO	Commvault	Carbonite	Druva	Code42 Crashplan
Solution Overview	Endpoint Protection, Security and Migration	Endpoint backup	Endpoint Protection	Endpoint data protection solutions	Data protection, management, and information governance	Endpoint Backup & Data Loss Prevention
Device & Data Inventory	✔	✘	✘	✘	✘	✘
Endpoint Backup	✔	✔	✔	✔	✔	✔
Local File Encryption	✔	✘	✔	✔	✔	✔
Remote Wipe	✔	✘	✔	✔	✔	✔
Device Geolocation	✔	✘	✔	✔	✔	✔
Data Theft Prevention	✔	✘	✘	✘	✘	✘
Full Remote Device Migration	✔	✘	✘	✘	✘	✘
Zero Knowledge Encryption Key Management	✔	✘	✘	✘	✘	✘
Hybrid Cloud Storage	✔	✘	✔	✔	✘	✔

Cibecs differentiators

Unlike many alternative products, Cibecs has been **purposefully built** for **simplified, scalable & secure business endpoints protection.**

Cibecs features specifically address the challenges associated with protecting user data on **endpoint devices**.

Discovery & Inventory

Cibecs enables the Discovery and Inventory of end user devices on the organization's network through a set of unique features that is designed to automatically discover and protect devices with minimal management. Data is classified into organizational & non organizational data to identify data at risk versus protected and provides a device Hardware and Software inventory.

Complete Central Management & Control

From granular **central policy setting**, allowing you to define what data to protect across all users, to being able to centrally enable encryption, remotely wipe or revoke data access**,** Cibecs is built for complete central **control over business endpoints**. The combination of features integrated into a single solution is part of what uniquely positions and differentiates Cibecs.

Simplified Reporting & Management

Cibecs has developed a **unique and different approach** to reporting across all users by providing the organization with a **single metric** known as the **Protection Rating** to monitor the effectiveness of Cibecs, and **protection against data loss** over thousands of users. The reporting system allows drilling down to see very specific user events. The Cibecs Control Centre provides multiple reporting metrics and allows for automated email reporting.

This reporting will prove compliance, as a result of the integrated backup and DLP feature set that Cibecs provides, to the end point data protection requirements set by the data protection legislation that governs your region.

Increased Operational Efficiency

First and foremost, Cibecs' is a security platform, however, the practical support features built into the platform provides IT with the tools needed to dramatically increase operational efficiencies in day-to-day data support scenarios. Deriving immediate return on investment and ensuring the platform a practical and self-funding tool.

Cibecs offers multiple operational benefits including **faster and simplified data migration projects** to new machines or operating systems, **reduced user downtime** in the event of data loss / ransomware attacks, and **improved IT service delivery.** The integration of PC migration and replacement features as part of a backup product was a concept that was pioneered by Cibecs.

Scalable Business Backup

Cibecs is easy to install to users and provides simplified central reporting by branch or by server. Cibecs allows for **scalable Remote Branch & Office Backup and** is easily scaled across organisations with multiple offices – supporting deployment in both a centralized and decentralized model while **preventing pressure on the network & inflated bandwidth costs.** Initial snapshots of branch office backups can be imported to assist with customer onboarding and **the Consolidated Dashboard and reporting** allows for unified reporting across multiple servers.

Data Loss Prevention

Cibecs offers **powerful additional features to protect your business data if a device is lost or stolen.**

Encryption

Cibecs completely protect files from unauthorized access by **securely encrypting the files on the user's computer.** By selectively encrypting data while excluding operating system files, Cibecs ensures minimal impact on user computers compared to other disk encryption solutions.

Remote Wipe

Remote Wipe enables your organization to **remotely delete** the data on a lost or stolen notebook, quickly & easily. Cibecs performs a **unique 3 phase remote wipe** process by first revoking access to the data ensuring a minimal data exposure window and subsequently performing both a delete and a secure erase of the data. This functionality is also very valuable when replacing hardware as old hardware can be wiped securely before being redistributed.

Data Theft Prevention

Data Theft Prevention, **a feature unique to Cibecs**, enables organizations to **automatically revoke user access to data after a set timeframe.** If a user's computer hasn't connected to the network for a defined period of time, the files on the device cannot be accessed. If a machine is lost or stolen, the files are automatically protected from unauthorized access. This eliminates the risk of brute force attacks.

Remote Revoke

Another unique feature, Cibecs allows access to files to be **remotely revoked in a non-destructive way** preventing a user from further accessing their files. This prevents data theft and increases your organization's protection against industrial espionage and is unique to Cibecs.

Geo-location

Cibecs' Geo-location functionality allows **the administrator to centrally locate any device** running Cibecs. If a device is not online at the time it will transmit its location the next time it is connected and communicates with the Cibecs server.

Cibecs Full Remote Device Migration

Our full remote endpoint migration service migrates all the user's data and profile settings while respecting security requirements. It enables you to follow best practices for your device migration projects and you can remotely migrate user data, profile settings, and more, in minutes.

Here's a brief overview of our main features:

Remotely trigger and monitor device migration

Migrations can be centrally triggered from Cloud Management and the migration status and progress can be monitored.

Full device-to-device migration

Device-to-device migration reduces the requirement for additional storage and migrates all files (including business and personal). The migration is encrypted as well as compressed to optimize the process and reduce impact.

Migrate all files and profile settings

All business and personal files for the user will be identified and seamlessly migrated to the new device. The user's computer profile including system and application settings are included in the migration.

Live migration

Migrations happen while users continue to work and when you are ready to hand over the device, simply do an update migration to bring across any new work or changes.

Key & Proprietary Technology

Scalable cloud architecture

Designed as a true multi-tenant cloud CQRS & event driven architecture with scalability on demand.

Patent-pending security

Patent-pending Zero Knowledge Encryption Key Management ensures enterprise grade security while storing data in the Cloud.

Cloud management

The system is managed in the Cloud while giving customers that option of on-premise or cloud storage enabling a path to the Cloud.

Convergent Encryption

Ensure the highest level of data security as data is de-duplicated across all users while maintaining separate decryption keys.

Proprietary De-duplication engine

Proprietary source-based de-duplication technology globally de-duplicates all data across the entire organization before transfer significantly reducing backup storage requirements.

Intuitive Protection Rating

Management and reporting across thousands of devices has been simplified through a single metric that provides insight into the organization's protection.