How does SecureCircle compare to other data security and access control solutions across three key IT considerations?

	Ease of Administrator Deployment	End-User Workflow Transparency	Depth of Security Coverage
Secure Circle Approach	 Easy to deploy and integrates with existing Identity and Access Management solutions.	 No change to user workflow; users and applications interact with protected data as normal.	 Cross-platform, file type agnostic and regardless of transport means or device used, access to data remains restricted.
Disk Encryption	 Easy to deploy but support issues caused by compatibility between encryption software and OS or backup software.	 No change to user workflow.	 Good protection against lost devices but not against human error, malware or hackers.
CASB	 Easy to deploy but potentially lots of one-time integration with various cloud apps.	 Users forced to login through gateway for all cloud apps.	 No security for files on local computer after downloading from cloud apps or any files created on the device.
File Encryption	 Have to manage encryption keys for all users and file access if not logged for alerts or auditing.	 Manual process to encrypt and decrypt whenever transferring a file. Requires users to make a proper decision.	 Files still decrypted during use and subject to human error, malware, hackers etc.
IRM	 Limits the applications users can access protected data.	 Manual process to secure individual files; doesn't scale. Restricts users to specific apps, file names, file size limits etc.	 Files still decrypted during use and subject to malware, hackers etc. Permissions are not retractable.
Data Loss Prevention	 Almost impossible to manage all egress points and devices. File access is not logged for alerts or auditing.	 Changes file names and extensions.	 Data only encrypted on egress and subject to malware, hackers etc. Permissions are not retractable.
UBA	 Easy to deploy and only requires monitoring file servers.	 No change to user workflow.	 Files not secured in any way; only alerts based on user behaviour. Data is subject to human error, malware, hackers etc.