



DATA SECURITY SOLUTIONS

HOW DOES AN IDENTITY-CENTRIC APPROACH COMPARE?

Discover how Secrutiny's Identity-Centric approach to data protection compares to other data security and access control solutions across three key IT considerations.



0203 8232 999
























enquiries@secrutiny.com



SECROUTINY



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

The cyber industry continues to be propagated by fear, uncertainty and doubt; but Securitiny focuses on the things that matter, helping organisations find a lasting solution to their security challenges.

Call us on 0203 8232 999 to discover how we can help you!

