What is Enterprise Digital Rights Management (EDRM)?

"EDRM is a core data-centric technology that tries to overcome these issues by focusing on the few aspects that are consistent and, to some extent, controllable. The user and the data processed by that user are all governed by a data-centric policy. Data-centric security protects data, ideally irrespective of its storage location, device and application. […] DLP prevents data leakage at the network or device edges. EDRM protects data beyond the edge and, if applied at creation, can cover the entire information life cycle." **[Gartner Report G00463697]**

	DLP	DRM
Objective	Prevent data leakage by controlling data distribution	Prevent unauthorized use by controlling user privileges for digital content
Technical approach	Agent-based control for storages (USB, file share), file transfers, output, email, etc.	File encryption, access control and privilege control (inside applications based on plug-ins)
Approach prerequisite	Data classification based on process context or data content	Data classification based on process context or data content
Technical support	Device and platform specific, application agnostic, file type specific in case of content classification	Device agnostic, platform & application specific, file type specific in case of content classification
Solution complexity	Limited solution complexity	High; requires automation for reducing complexity
Protection effectiveness	Inside of controlled IT environments (on endpoint devices with DLP agent installed and DLP protected cloud services)	On all devices and IT / cloud environments regardless of the infrastructure security
Security controls	"Binary" (allow or block the action)	Granular access and privilege control (view, edit, copy, print, export, etc.)
Security controls (incl. change) after data sharing	No	Yes
Usage fault tolerance	Limited (e.g. immediate breach when a file is sent to the wrong recipient or when using copy & paste)	Robust (user can have the file, but it is useless without access authorization; copy & paste is covered by the privilege control) even in case of ransomware attacks
GDPR compliance	No (no forwarding control)	Yes (using access expiration date is required)

Reference:
1. https://secude.com/enterprise-digital-rights-management/

SECUDE