

Seclore for Media and Entertainment Companies

Lights, Camera, Security!

The Media and Entertainment industry is experiencing tremendous growth, fuelled by increasing digitization, increasing demand for content, and a growing consumer base. Sadly however, the industry, like many others, remains dangerously relaxed about data security. Witness the ease with which the Sony hack was executed. Sensitive information about Sony's clients was lying around unencrypted and unprotected. Executive's emails were easily accessed and exploited. As was clearly shown, such hacks dent not only corporate and personal reputations but also bottom lines.

Seclore's Enterprise Rights Management solution secures information in a file-centric manner. Access to data stored in files (over 60 file formats are supported) can be controlled wherever the file travels. Persistent, file-centric security reduces the dependency on different security solutions to secure information as it moves across different environments. Take the example of a draft script being emailed by the original writer to an agent. The agent will download the script to their laptop. From there the script may be circulated across various teams, stored on a network folder, and perhaps sent via a file-sharing service to a producer or studio. Once that script leaves the original writer's desktop, it can be accessed by anyone, shared with anyone, or easily accessed if any of the devices are stolen.

Seclore's ERM protects files throughout the collaboration life cycle. The document owner can automatically enforce exactly who can view the file, what they can do

with the file (edit, print, screen capture etc.), from which device and for how long. Here are a few examples of where Media and Entertainment companies are using persistent file security to protect their corporate value:

Protecting Scripts:

While the casting of a film is being determined, the script needs to be sent to various actors (via their respective agencies) for consideration. Physical copies of such scripts can be easily leaked by any one of these parties to the press even before the roles have been cast. Digital copies are even easier to leak – you just need to forward the email to a journalist.

To protect this intellectual property, leading Media companies are securing these scripts with Seclore's ERM before they are sent to other third parties. Since only 'read access' is required, the agents and actors do not even need to install any software – they can simply use Seclore's browser-based viewer to read the protected script.

Securing Production Collaboration

Concept notes, production updates, draft revisions, and marketing plans are circulated internally (and externally) across various teams involved in a production. These files are typically shared via email or filesharing services during the production process. While these documents are meant to be strictly confidential and their circulation extremely restricted, the high volume of files and emails – combined with

the large number of people involved in the production process – makes data leakage almost inevitable.

With Seclore's ERM, all documents are protected before being circulated. All copies created (including annotated and edited copies) and all subsequent drafts also remain protected. Nobody except authorized users can access this information. Thus, the chances of a script or other sensitive aspects of the production being leaked to the public are virtually eliminated.

Keeping RFPs and Tender Documents Secure

To recruit various vendors for production and post-production activities, companies release some highly confidential information as part of the vendor evaluation and RFP process. The company has no visibility over the documents once they are sent to the bidding parties. Any of these bidders can potentially leak this data – to the public and to competitors. The Non-disclosure Agreement (NDA) signed with the bidders is utterly useless to actually prevent data misuse by the bidders – voluntarily or maliciously. The documents are sent to bidders and interested parties in protected form. Only designated employees within bidding organizations can access these documents and all access to the data is centrally logged. based viewer to read the protected script.

USA – West Coast

691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

USA – East Coast

420 Lexington Avenue
Suite 300,
Graybar Building
New York City
NY 10170

India

Excom House Second Floor
Plot No. 7 & 8,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072

+91 22 6130 4200
+91 22 6143 4800

Gurugram

+91 124 475 0600

Singapore

Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton
Way
Level 34-01
Singapore – 068811

+65 8292 1930
+65 9180 2700

Europe

Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 151 1918 5673

UAE

Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

Saudi Arabia

5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

