Securing Data in the Era of GenAI and LLM Technologies

A conversation with…

Mark Sutera
VP, Enterprise Sales
Seclore

Tom Dunlap
Managing Partner
DIACSUS

Jay Como
Head of Enterprise Data Governance and Operations
T. Rowe Price

Mark Davies
Partner
Element22
Today’s panel

**Moderator**

Jim Halcomb  
Global Head of Research and Development  
EDM Council

Mark Sutera  
VP, Enterprise Sales  
Seclore

Tom Dunlap  
Managing Partner  
DIACSUS

Jay Como  
Head of Enterprise Data Governance and Operations  
T. Rowe Price

Mark Davies  
Partner  
Element22

© 2022 EDM Council Inc.
The Evolution of GenAl and LLM Technologies...1/3

There is a strong need for ensuring data completeness and data quality, while protecting sensitive data.

For 2024, Artificial Intelligence (AI) usage is evolving significantly with variants for Generative AI (GenAI) and Large Language Models (LLMs) to drive data intelligence offerings and automation tasks that include:

- Text generation
- Language translation
- Content summary
- Rewriting context
- Classification and Categorization
- Sentiment analysis
- Conversational chatbots

The proliferation of this technology is upon us now and likely to stick around for a long time.

Much of this technology is being applied for the betterment of data intelligence integrity, workflows, and processes. Yet there are inherent business drivers worth looking at to ensure good applications of the technology for data completeness, timeliness, accuracy, and security.
The Evolution of GenAI and LLM Technologies... 2/3

Relevant business drivers and considerations for protecting sensitive data, when applying GenAI and LLM Technologies.

Interpretations of Data Use Cases: the marketplace wants to know about data changes real-time; doing so is not necessarily a binary or linear process. Often interpretations are subjective or discretionary across data use cases, for example, with principle-based policies or regulatory rules. These involve applying GenAI and LLM technologies to perform such interpretations correctly, checking for the relevant and right data types and their content, conducting language translations, and stitching the data together sensibly and accurately.

Change Management: Being able to reconcile data types and content across the use cases must be done efficiently and effectively, while protecting the data, e.g., access rights and visibility. AI technologies help master these activities via comparative analyses while recording decisions for future reference on use cases.

Workflow automation: the resulting outcomes of GenAI and LLM enabled and tracked data changes are expected to lead to more automation in data workflows while knowing, controlling, and protecting the data, e.g., eliminating previously manual tasks while being conformant to data privacy rules.

Strong data lineage: having good traceability and data lineage is key for understanding changes made systemically using AI based technologies on a historical basis in the event that there are data, rule, change management, or other types of discrepancies.
The Evolution of GenAI and LLM Technologies... 3/3

With the proliferation of AI technologies applied in data intelligence, there are important safeguards to consider for mitigating risks that are high on the radars of regulators and marketplace participants alike.

Being in violation of a regulation:
• Ensure strong set of repeatable checks and balances on data interpretations and protections.
• Run changes in a prod parallel environment with UAT.
• Perform regression testing in prod post code deployment.

Lack of staff awareness and training:
• Ensure staff are trained on the data types and use cases.
• Have a capable Business Analysis function for data applications, interpretations, and protections.

Poor perception with using GenAI and LLM technologies to manage data activities across mandated functions, e.g., regulatory reporting:
• Proactive marketplace awareness of the benefits for using the technologies.
• Promoting the best practices and controls of a data-centric security solutions suite linked to the GenAI and LLM technologies and their related data use cases.
Questions?
Protecting the world’s sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance.

**Trusted & Proven**

> 40 Million documents and emails protected each month across 2,000+ global customers.

**Global Support**

Deployed in 60+ countries with offices in six countries.

**Pervasive**

Relied on by organizations in every vertical, including financial services, manufacturing, and government.

---

### Sampling of Customers

- AMERICAN EXPRESS
- ICICI Bank
- flex
- L&T Infotech
- CHENIERE
- vodafone
- GM
- GM FINANCIAL
- Ford

---

<table>
<thead>
<tr>
<th>Overall Rating</th>
<th>89% willing to recommend</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5/5 (53 Reviews)</td>
<td></td>
</tr>
<tr>
<td>5 Star</td>
<td>57%</td>
</tr>
<tr>
<td>4 Star</td>
<td>43%</td>
</tr>
<tr>
<td>3 Star</td>
<td>0%</td>
</tr>
<tr>
<td>2 Star</td>
<td>0%</td>
</tr>
<tr>
<td>1 Star</td>
<td>0%</td>
</tr>
</tbody>
</table>
WHY SECLORE?

- PROTECTION (AES 256)
- ACCESS CONTROL
- DYNAMIC WATERMARKING
- GRANULAR USAGE CONTROLS
- CLASSIFICATION VISUAL LABELING
- TIME BASED CONTROLS

- LOCATION BASED CONTROLS
- DYNAMIC POLICY FEDERATION
- REAL TIME ACCESS REVOCATION
- ACCESS PATTERNS & ANALYTICS
- RISK INSIGHTS & TRENDS
- GEO LOCATION AWARENESS
Seclore has global customers, including large brand name enterprises, that rely on Seclore’s data-centric security platform.
Join EDM Council and our membership community of companies…

Global Advocates for Data & Analytics Management

The leading global trade association providing best practices, standards and education to data and business professionals in our data-driven world.

edmcouncil.org
Thank you!

FOR MORE INFORMATION:
Mark Sutera
VP, Enterprise Sales
Seclore
mark.sutera@seclore.com
Call 617-872-1305