Bloor InBrief

Daniel Howard – Analyst

SOLIX®
Empowering the Data-driven Enterprise

www.solix.com

4701 Patrick Henry Drive, Bldg 20
Santa Clara, CA 95054, USA
Tel: +1 (408) 654 6400
Email: info@solix.com

Solix Common Data Platform (CDP) for Data Governance

The company

Solix Technologies is a software vendor that specialises in Enterprise Information Management. It was founded in 2002, is headquartered in Santa Clara, CA, and has more than 250+ employees across the US, Europe, Australia, India and Dubai.

What is it?

Solix Common Data Platform (CDP) is a broadly applicable 'Big Data Application Framework' (see ***Figure 1***) that provides an information architecture for your data-driven enterprise to manage, govern and leverage all of your enterprise data. CDP is accessible through the web browser, can be deployed in-cloud or on-prem, and operates at big data scale across both structured and unstructured data.

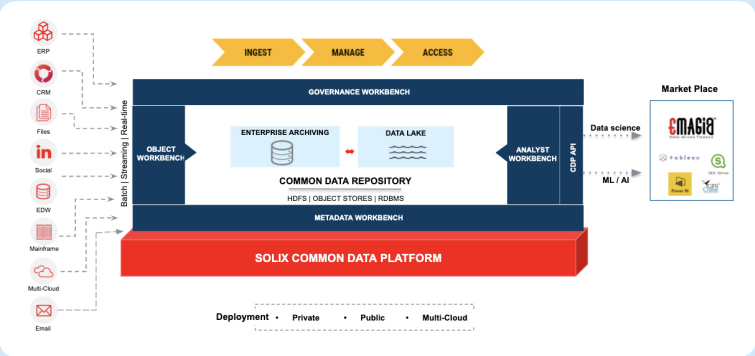


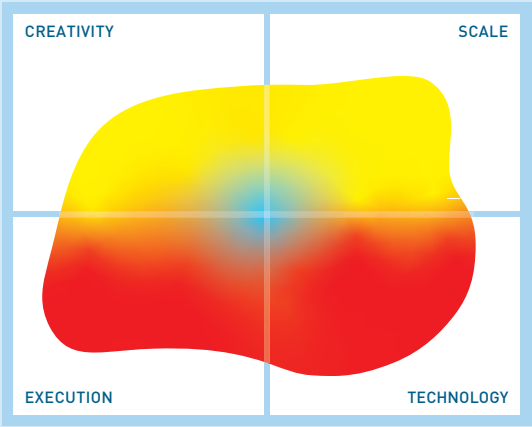
Figure 1 – *Solix Common Data Platform*

What does it do?

CDP provides a wealth of data governance capabilities, including a business glossary, data discovery, data security, data classification, data access, data masking, dashboarding, role management and role-based views, workflows, approval processes, policy management, search access to your data and metadata, data profiling of both internal and external systems, and so on. What's more, these capabilities invariably come with additional features and nuance: for example, the product can classify your data during ingestion; its sensitive data discovery comes with a dedicated dedicated data privacy compliance tool that addresses GDPR, CCPA and similar regulations; and it leverages a number of external security technologies, such as LDAP and single sign-on, as part of its data security functionality, and can integrate with a number of third party security products using these technologies.

In addition, CDP allows you to build data landscapes that visualise the data within your system, either in whole or in part. At present, the creation of these landscapes requires some manual intervention, although we are told that there are plans to fully automate the process in upcoming releases. It also allows you to store and manage technical data and metadata as well as accompanying business meanings and interpretations. This is useful for enabling widespread understanding of your technical data assets, and particularly so when that data is poorly self-described (for example, a field named *"column_1"*).

All that said, the product's most significant differentiator is in how it approaches Subject Access Requests (SARs), data retention and the right to erasure (colloquially the 'right to be forgotten'), driven by regulation such as GDPR, CCPA and other compliance mandates. To start with, the product provides a dedicated space for managing your SARs, and allows you to leverage identifying information (ID numbers, for instance) within them to scan your data



The image in this Mutable Quadrant is derived from 13 high level metrics, the more the image covers a section the better. Execution metrics relate to the company, Technology to the product, Creativity to both technical and business innovation and Scale covers the potential business and market impact.

Metadata management	★★★½	Business orientation	★★★★
Policy Management and Regulatory Compliance	★★★★½	Ease of use	★★★½
		Collaboration and data democratisation	★★★

landscapes for all relevant data. You can also export this data in a compliance report, generated in either PDF or Excel format. This makes it much easier to find and provide information related to a given individual within your system, and hence satisfy their SAR.

For structured data, data retention is handled by either purging or obfuscating personal data when the need arises. This could be on-demand (for example, if the right to erasure is leveraged) or simply due to time elapsing and the retention period for that data expiring. In any case, when the user consent ends and the legal retention process starts, the data in question is immediately archived from the primary source, which stops it from being used in any future unauthorised processing. Purging data is accomplished through the use of purge configurations, which contain criteria used to identify which data to purge as well as a flowchart that determines which tables to purge in (shown in ***Figure 2***). Obfuscation, on the other hand, is accomplished by applying masking rules.

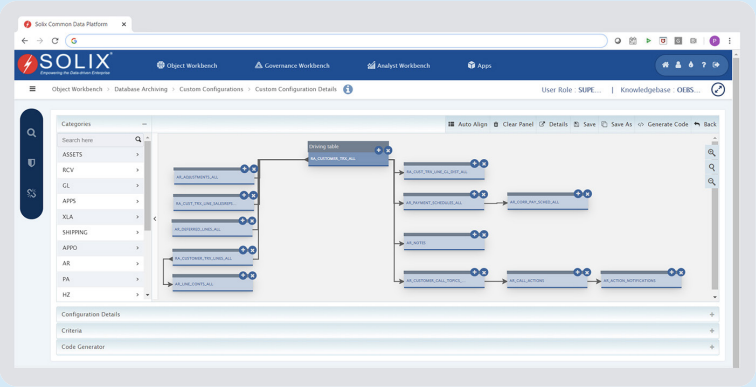


Figure 2 - *Purge Configuration*

For unstructured data (specifically, documents) the process is much the same, except for the fact that redaction can be employed rather than purging or obfuscation. As you might expect, this entails obscuring specifically the expired or erased personal data within your documents, leaving the rest of the document intact. Purges, obfuscations and redactions are logged, as are all operations, and they can be run in batch.

You can also automate the removal of expired data using retention policies. For instance, you could define a policy that automatically assigns a retention period to your data based on various criteria, then automatically purge that data using an associated, workflow-driven purge configuration when its retention period is over. Retention policies apply to your data automatically and retroactively, meaning that they a) apply appropriately to data that should already be partway through their retention period and b) can automatically purge data whose retention period has already lapsed. If necessary, you can also apply 'legal holds' to your data, preventing the affected data from being purged while the hold is active. Notably, this will not freeze that data's retention period, meaning that it can still expire while the hold is in effect, but it won't be purged until the hold has been removed.

Why should you care?

CDP is a single, unified platform that provides access to everything you need for governing your data in a single location. It's fit for purpose, particularly in regard to data lakes, and is well suited for handling compliance in a world where regulatory requirements are both frequently changing and differ dramatically from country to country and region to region.

Its capabilities surrounding data retention are particularly impressive. For starters, it has clearly been built with data privacy regulation, such as GDPR and CCPA, in mind, and it is very well suited to addressing the right to erasure. More than that, it is clear that its retention process is highly flexible and configurable. It enables you to take a dynamic view of retention, where data may need to be retained for different periods and disposed of in different ways based on both your own requirements as an organisation and a variety of different regulatory mandates with which you need to comply. Given that many nations and regions (US states, in particular) are busy defining their own legislature for personal data, which will rarely match up perfectly with GDPR and CCPA (and in some cases may diverge significantly), this is a very useful capability now that is likely to prove even more useful in the future.

The Bottom Line

Solix CDP offers end to end functionality for data governance and beyond, with particular emphasis placed on big data as well as regulatory compliance in general and data retention in specific. If you care about these areas – and there are many reasons you should – it is more than worth a look.

FOR FURTHER INFORMATION AND RESEARCH CLICK HERE