SPIRION

SOLUTION OVERVIEW

Tonic's integration with Spirion

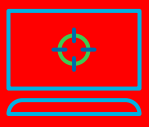
Spirion, a pioneer in data protection and compliance, understands that true data privacy cannot be achieved by a single solution, and instead, requires an ecosystem of purpose-built technologies working together to fill any potential gaps in a privacy program. It is to that end that Spirion has added Tonic to its already strong platform of privacy and security solutions. Tonic complements Spirion replacing sensitive information found within datasets with de-identifiable or synthetic data.

Security and risk management leaders are now able to respond to requests for PII (Personal Identifying Information) data removal, while maintaining the business value of their data and adhering to regulatory compliance, (CCPA & GDPR) through the unique relationship between Spirion and Tonic.

Additionally, the solution provides a mathematically provable guarantee of privacy protection against a wide range of privacy attacks, including differencing attack, linkage attacks, and reconstruction attacks.

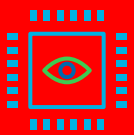
Further, the database structure, as well as business continuity and company performance are not affected. Businesses are also able to utilize Tonic as a test environment, by testing their production environment without compromising their own data. The data would simply be replaced with synthetic or de-identifying data for testing purposes.

De-identification of data can protect against attacks that include:



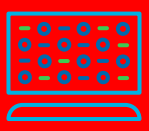
Differencing Attack

A Differencing attack uses background knowledge about an individual person to learn sensitive information about that person by taking into account multiple statistics in which the target's data was included.



Linkage Attack

A linkage attack attempts to re-identify individuals in an anonymized dataset by combining that data with another dataset.



Reconstruction Attack

A reconstruction attack is any method for partially reconstructing a private dataset from public aggregate information. Typically, the dataset contains sensitive information about individuals, whose privacy needs to be protected.

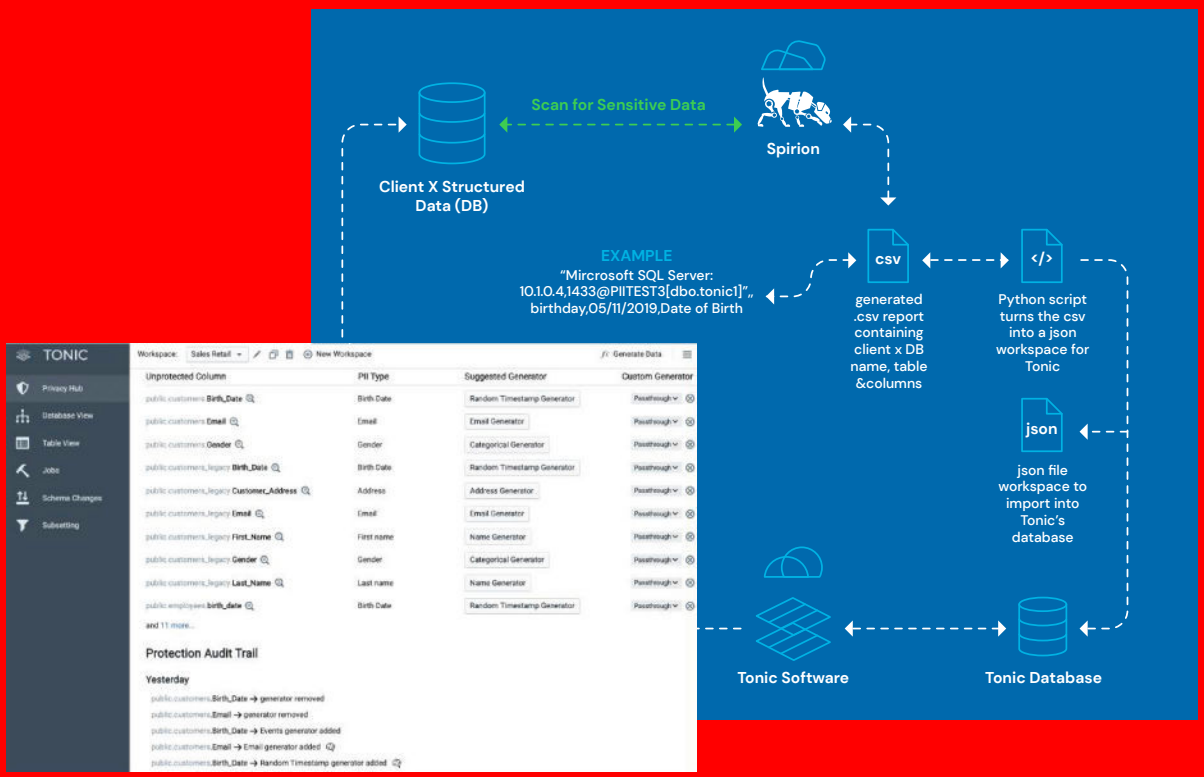
Solution Benefits

Spirion's proprietary AnyFind™ technology scans an organization's fileshares and databases, on premise and in the cloud, for information that can include such data as: Names, Birthdates, Addresses, Payment Card Information, Email, or any other types of personally identifiable information (PII). Once discovered, Tonic is able to replace the PII with synthetic data to remove any connection with any individuals contained within without stripping the data of its business value.

The integration enables users to secure identity-centric data, apply the right to be forgotten, and ensure the lawful processing of data by removing all traces of PII without compromising data integrity. The solution is mathematically proven to protect against a wide range of privacy, differencing, linkage, and reconstruction attacks.

Differential privacy makes it possible for organizations to securely share de-identified data with others who would not usually have access to it, such as marketing for analytics and trend tracking, giving them deeper insights within the context of their business. The technique also benefits IT teams by letting them test production environments and automate data modeling using de-identified synthetic data without compromising their data.

Tonic & Spirion Data Flow



Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion is the leader in data discovery, persistent classification, and protection of sensitive data on-premise and in the cloud. Since 2006, thousands of organizations worldwide have reduced their sensitive data footprint and proactively minimized the risks, costs and reputational damage of successful cyberattacks. Spirion provides greater command and control of sensitive data to leading firms across all industries from financial services to healthcare to public sector. Visit us at spirion.com