SPOTLIGHT

Sponsored by: Anonos

Data mobility is critical to get value out of data, so constraining data within four walls is no longer effective. Performant privacy–based controls are independent of parameters and travel with data, strengthening privacy and increasing value.

Accelerating Data Control for Economic Value

September 2023

Written by: Stewart Bond, Vice President, Data Intelligence and Integration Software

Introduction

To compete as a digital business in the modern economy, organizations need to be intelligent enterprises. Organizations with high levels of enterprise intelligence experience three or four times better business outcomes as compared with organizations with low levels of enterprise intelligence. Intelligent enterprises make decisions faster, and they better manage revenue, cost, and risk in the face of rapid change and a need for adaptation.

Building enterprise intelligence requires the ability to synthesize information, deliver insights at scale, support collective learning, and foster a data culture. The foundation of enterprise intelligence is data, and a common thread that runs through enterprise intelligence capabilities is effective, timely use and sharing of data. But the complexity of modern data environments that are highly distributed, diverse, and dynamic — coupled with complex and rapidly changing regulatory requirements — requires controlled data sharing to ensure privacy compliance and suitability in the context of business problems being addressed. Moreover, many organizations have realized that if their internal enterprise data is combined with external data, they have greater monetization possibilities to improve customer experience, create better products and services, protect against risk, and expand rapidly. However, they are held back by rapidly evolving data privacy and regulatory concerns. Data security and privacy are no longer just the responsibility of the CISO but are quickly becoming the responsibility of chief data and/or analytics officers (CDAOs). As CDAOs are tasked with getting value out of data, they also manage data governance, ensuring that data is being used appropriately and is properly protected and compliant with all regulations.

AT A GLANCE

KEY STAT

Improvements in enterprise intelligence can be tripled or quadrupled by focusing on privacy mitigated economic value.

WHAT'S IMPORTANT

The foundation of enterprise intelligence is data, and becoming an intelligent enterprise requires effective, timely use and sharing of data to accelerate decision making and business value.

Data controls have historically assumed that data is all in one place, but data mobility is critical to get value out of data, so holding it back within four walls is no longer effective in modern data environments. Traditional methods such as encryption, tokenization, and masking protect data at rest and in transit, but they don't protect data while being processed. Selecting the method to protect data during processing requires anticipating different use cases of the data prior to consumption, which is not possible by using traditional protection methods in modern data environments, because the rate of distribution, diversity, and the dynamics of how, where, and when the data is used and who uses it is constantly changing.

Stakeholders are often hesitant to share data because of compliance constraints. Secondary processing of data may not be lawful if controls were designed to protect the data for only one type of use case, and international data transfers may not be feasible if sovereignty restrictions exist. In the IDC's February 2023 *Future Enterprise Resiliency Survey*, only 33% of the 952 organizations surveyed globally believe they are fully compliant with data sovereignty laws, and the numbers significantly lower in Europe and Asia/Pacific. Data is an enterprise asset, so it needs to be shared. But without performant privacy (as described in the section that follows), applying controls before knowing how the data will be used causes futility instead of utility.

Protecting data through the full life cycle, from rest to consumption, also requires considering the ability of bad actors to identify individuals using the mosaic effect. This method can reidentify parties (e.g., individuals or companies) by combining seemingly anonymized or deidentified data with other information that is available. Privacy protection in modern data environments must extend beyond individual data sets and recognize the relationships among and across data sets to eliminate the possibility of reidentifying parties by using the mosaic effect.

Performant privacy–based controls are independent of parameters and travel with data as it is shared within the enterprise, within its extended ecosystem, and across international borders. Reconciling data protection and utility will accelerate data to decision, increase the value of data in digital business, and in some cases, create new data-based revenue streams.

Benefits of Performant Privacy–Based Controls

Performant privacy is state of the art for retaining the performance characteristics of unprotected source data (such as speed of processing, accuracy, and fidelity) while improving privacy to satisfy compliance requirements. Performant privacy–based controls protect data wherever it is used by embedding high-utility, fit-for-purpose privacy controls into the data so that it processes and performs with the same characteristics of speed and accuracy as unprotected data. Performant privacy–based controls reconcile data protection and utility, unlock data flows, and reduce data compliance risks, thereby increasing data value without impeding the timely access and use of data for accelerated decision making and business value.

The benefits include:

- Faster time to value by eliminating project delays related to data privacy and compliance issues
- Cost-effective protection through automated application and enforcement of enterprise standards
- Improved data sharing, combination, and use by facilitating international data transfers without risk
- Reduced data hoarding within the organization
- Removal of the mosaic effect, enabling lawful secondary use
- Automation of ad hoc privacy engineering without risk
- Helping stakeholders overcome hesitancies to share data
- Reduction, if not elimination, of data breach liabilities

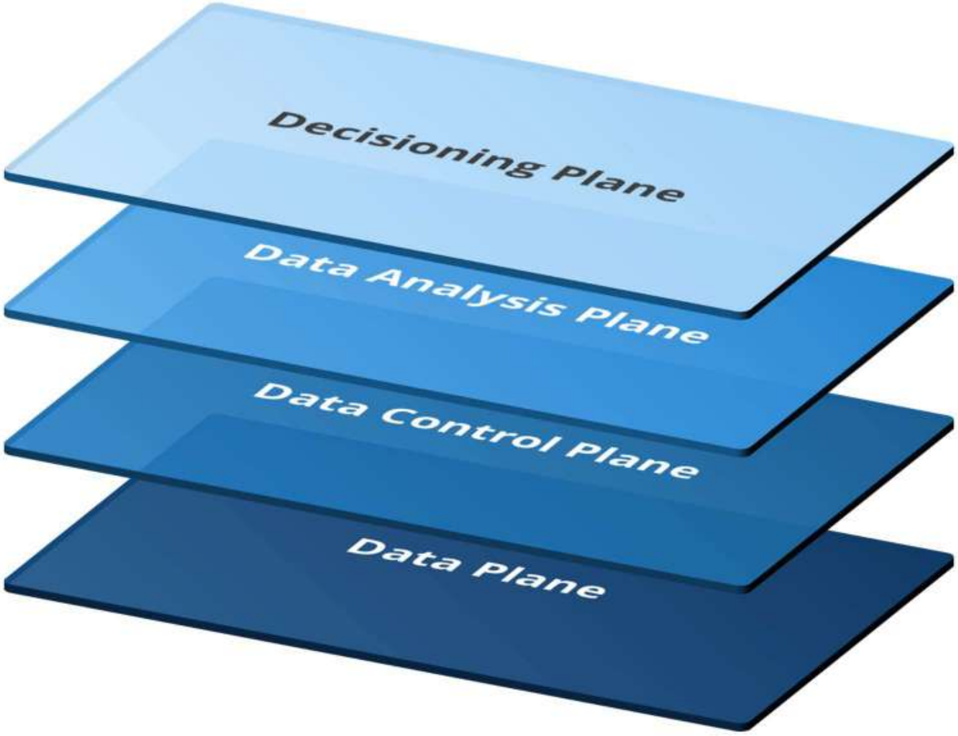
Without performant privacy–based controls, an organization's ability to become an intelligent enterprise is restricted and will thus be held back from achieving three or four times higher levels of financial and operational business outcomes.

Trends

Generative artificial intelligence (AI) is ushering in a new era of intelligent automation. Generative AI has simultaneously captured the attention, imagination, and concern of most tech and business leaders worldwide, and a new platform is emerging to support new use cases. This new platform is not one built on hardware; it's a platform that is changing our relationship with data and how we extract value from data. As our relationship with data changes, we still need to ensure proper and appropriate use while remaining compliant with data laws and regulations. There have been inherent privacy issues with artificial intelligence trained by machine learning (ML) for some time. Generative AI and large language models (LLMs) are amplifying the risk and opportunities of ML because they dramatically democratize access to the insights derived from ML. Performant privacy can protect against prompt leakage of proprietary context or data and can safely train domain-specific LLMs.

As organizations rush to the cloud in data modernization initiatives, they are looking at the storage, management, usage, and sharing of data as separate functions. Few organizations have a comprehensive enterprise intelligence strategy with the corresponding architecture that can truly improve the metrics that matter. As shown in Figure 1, IDC sees the need for four planes of capabilities to enable enterprise intelligence: a data plane, a data control plane, a data analysis plane, and a decisioning plane.

FIGURE 1: ***The Four Planes of Enterprise Intelligence Architecture***



Source: IDC, 2023

Data that resides in the data plane is controlled by the plane above it, which is leveraged in analysis that drives insights for decisions. Performant privacy can ensure the correct and compliant use of data from the bottom to the top of the architecture, shed light on dark data that cannot normally be activated because of privacy concerns, and remove data privacy risks to confidently build higher levels of enterprise intelligence.

The number of regional data regulations continues to grow, with each new regulation getting tougher on organizations that manage sensitive information about people, places, and things. The biggest issue many organizations face is that they usually know the original source of the data but not where every copy of the data is. Organizations are accountable for the original source of data and every copy. Performant privacy enables changing regulations into automated data protection controls so that organizations stay abreast of the ever-evolving requirements.

Considering Anonos for Performant Privacy–Based Controls

Anonos Data Embassy software uses performant privacy–based controls to reconcile tensions between ensuring high data utility and effectively protecting data when it's used between and outside of parameters. The benefits of the solution include the following:

- **Accelerates speed to access**: Anonos Data Embassy software provisions protected versions of preapproved data sets, making them immediately available for compliant processing by leveraging:
  - Centralized control over decentralized processing
  - Automation of scarce data engineering and privacy expertise
  - API, low-code, and no-code support for the full range of users
- **Creates protected versions of sensitive data:** Anonos Data Embassy software leverages multiple data protection techniques to create new compliant and approved use case–specific protected versions of data called "Variant Twins." These use case–specific variations of digital twins embed controls that remove obstacles to processing by protecting the data during computation to deliver:
  - Artificially generated data for testing and development
  - Permanent or reversible redaction of personally identifiable information (PII) in unstructured text
  - Synthetic data to augment incomplete data for model development
  - Reversible lawfully deidentified data for model production use

Anonos also has a synthetic data generation capability. Organizations can artificially generate data that mimics production data's structure and statistical properties. Synthetic data can be used for testing and training, thus eliminating privacy risks in software and analytical model development.

Anonos is enabling data modernization by helping organizations turn privacy and compliance roadblocks into on-ramps to digital business.

Challenges

Anonos can be incorrectly lumped in with many different data security and privacy software vendors. Anonos has a big task to educate the market on how its implementation of performant privacy–based controls is different and what value it adds to ensuring compliant sharing and consumption of data at all levels of sensitivity.

Conclusion

Organizations wanting to compete as a digital business in a digital economy need to be intelligent enterprises, and intelligent enterprises need to be able to accelerate the control of data to realize economic value without risk. Performant privacy–based controls can help organizations overcome privacy hurdles, share and utilize more data, and improve the economic value realized from data. Anonos' implementation is differentiating, and to the extent that it can address the challenges described in this paper, the company has a significant opportunity for success.

Performant privacy–based controls can help organizations overcome privacy hurdles, share and utilize more data, and improve the economic value realized from data.

About the Analyst

Stewart Bond, *Vice President, Data Intelligence and Integration Software*

Stewart has led numerous research projects and publications and is recognized as a valued industry analyst by leading software vendors, consumers, and peers in the areas of enterprise and data integration, business-to-business integration, Big Data, and cloud. Prior to becoming a market and industry analyst in 2011, Stewart spent 10 years with IBM as a master certified IT architect, consulting on information management and middleware strategies and delivering integration solutions to customers around the globe.

MESSAGE FROM THE SPONSOR

Anonos eliminates the conflict between data protection and utility that is holding the industry back from accelerating data control for economic value, including fully leveraging AI:

- We do this by enforcing performant privacy controls that ensure that the inherent characteristics of original, unprotected data, such as processing speed, accuracy, and fidelity, remain intact, all while ensuring compliance with the most rigorous global privacy and security standards when the data is in use.
- Our Variant Twins secure data during processing wherever it flows — within an organization, its broader network, and across organizational and jurisdictional borders.
- By merging data protection with utility, our globally patented Data Embassy software amplifies the value of high-risk data (like PII, personal data, and trade secrets) to pave the way for innovative new AI-driven insights and revenue.

Learn more about empowering faster, broader, and more consistent use of data to improve business outcomes at www.anonos.com

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.