Publication date:
21 Apr 2021
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: TripleBlind enables secure data sharing for third-party processing

Brought to you by Informa Tech

Table of Contents :

Summary 2
Market context 2
Product overview 3
Company information 4
Analyst comment 6
Appendix 6

Summary

Catalyst

TripleBlind develops technology that enables organizations to submit their data securely to a third-party processor in order to use the latter's algorithms for the purpose of analysis, algorithm training, or other computations.

Omdia view

Healthcare is the place where third-party analytics delivered on securely private data has so far generated the most immediate interest, to the point where that sector has even come up with the concept of *data liquidity*, which is yet to gain currency in other verticals. That said, tech such as TripleBlind's is clearly relevant elsewhere, as its financial services customers demonstrate. Government and retail spring to mind, and of course, the algorithm providers, whether in commercial entities or academia, should also be interested in technology that enables them to work on data whose owners can (a) rest assured it cannot be decrypted and (b) put strict limits on what computations can be performed on it.

As to the competitive landscape in which TripleBlind finds itself, clearly there are tech heavyweights behind the other three approaches outlined in this report. The new kid on the block will need to partner with a major name or two for visibility and market access. However, if it can sign up and publicize enough high-profile customers (Tier 1 banks are always good), it might even attract the attention of another industry major and be acquired, which could certainly shift the competitive balance in this emerging market.

Why put TripleBlind on your radar?

TripleBlind addresses many of the shortcomings of the other approaches to data privacy for third-party processing. Its pricing mechanism, which factors in the size of the company, makes it attractive to customers large and small, as does the ability to start with just two counterparties then expand as needed once your comfort level grows.

Market context

The problem space TripleBlind came into existence to address is that of enabling one organization (or to use GDPR terminology, a data collector) to submit its data in a secure fashion to another (i.e., a data processor, which in this case would be the supplier of an algorithm) for analysis in the cloud. While the sender can store and transmit the data in encrypted form, as soon as the recipient decrypts it for purposes of processing, an unacceptable element of risk is introduced.

This issue has arisen of late because analysis of big datasets can achieve unique insights, that is, ones that analysis of smaller sets simply cannot surface. This is particularly important in certain fields such as healthcare, where analysis of the data of millions of patients can indicate general trends in an entire population or in particular demographic groups.

Indeed, a term has arisen in that sector, namely *data liquidity*, which borrows from economics, where an asset's liquidity is measured by how readily usable it is: cash is the most-liquid asset, whereas a long-term

savings account is essentially illiquid, in that it is tied up and unusable for that period. With data, therefore, its ability to be used without risk of compromise is its liquidity, and though it originated in healthcare, the term has the potential to be applied in virtually any area of activity in the private or public sector.

In the case of healthcare, this requires technology to protect the privacy of individual patients and the actions taken on behalf of patients by their families or medical staff. There is already risk in a second party (i.e., the data processor) seeing the data, and this is only compounded by the fact that it is often better to use clinical data from multiple hospitals and run the analysis centrally to achieve optimal insights, bringing many more parties into the equation.

Various technological approaches have arisen to address this challenge. In recent reports (see **Further reading**) Omdia has highlighted three:

- **Homomorphic encryption**, which enables computations to be performed on encrypted data without first decrypting it
- **Confidential computing**, which leverages trusted execution environment (TEE) (a.k.a. secure enclave) technology on semiconductors, also known as secure enclaves, such that encrypted data can be decrypted and processed exclusively in the enclave, thereby limiting access to ensure that data in use is protected
- **Differential privacy**, whereby bogus data (a.k.a. noise) is introduced into a dataset, such that individuals cannot be identified but the data can still be used for analytical computations

Product overview

TripleBlind's technology is an alternative approach to the three mentioned above and is complementary to at least one of them, namely confidential computing, in that it can deliver the encryption/anonymization capability that confidential computing itself does not.

It works by installing a Docker container with its code within the infrastructure of both the data collector and data processor. On the collector's side, the data is de-identified. It is then encrypted via a one-way transformation, rather like a one-way hash but nondeterministic. This means it cannot be reverted to its original state by the recipient (i.e., there is no decryption possible) but can be submitted to computations. Indeed, data encrypted by TripleBlind can never be decrypted and will never need to be, since it can be used as it is for any computational requirement from regular processing to statistical or neural network training.

The processor uses the TripleBlind container in its infrastructure to manipulate the data without decrypting it. Permission for the use of that data can be restricted by the collector to one specific computational process. That is, the processor cannot reuse it or subject it to any other type of action, enabling TripleBlind to tout its digital rights management (DRM) capabilities. In addition, on the processor's side, the algorithm itself can be encrypted for a further level of security.

The encryption technology used by TripleBlind, which it calls Privophy, works across text, voice, and graphic content and supports nonlinear operations, including comparisons. The vendor says the system has "tens of thousands" of bits of entropy compared with, for instance, 256 for AES256. This situation enables it to claim far greater quantum resistance, that is, the ability to withstand the onslaught of quantum computers, which will be able to crack many of the cryptographic ciphers currently in common use.

Each of the proposed methods of achieving privacy for data that is shared with a third party for some form of computation has its advantages and shortcomings, and different tech groups advocate each:

- **Homomorphic encryption** tends to be quite slow and is very compute intensive, which currently limits considerably its addressable market. This explains why one of its key proponents, IBM, offers homomorphic encryption as a cloud-based service leveraging its own considerable compute infrastructure. The technology also does not work on audio or video data. In terms of the actions available to companies using it, it supports additions, subtractions, and multiplications, beyond which its use becomes more complex, and it has no DRM capability: once the data has been delivered to the processor, the collector has no control over any other uses that the latter may put it to. There are also academic debates about whether homomorphic encryption is quantum resistant. Smaller vendors in this segment include Duality Technologies and Enveil.
- **Confidential computing** is championed by the likes of Intel (with its SGX secure enclave technology) and other chip manufacturers. One issue is that it does not address the issue of data anonymization as required by medical regulations such as HIPAA and GDPR. Also, since it is hardware dependent (i.e., it relies on the presence of the TEE on the underlying silicon), it usually requires all the data to be brought together in one physical place (i.e. wherever the processing is to take place), which may fall foul of regulations such as GDPR in certain geographies. Because it is hardware based, systems cannot be remotely updated.
- **Differential privacy** is favored by some players in the big tech arena such as Google and Apple. It works well for tabular data but, again, cannot operate on audio or video files and is thus not suitable for applications such as fraud prevention or the analysis of healthcare records because it adds “noise” (i.e., wrong or irrelevant information) to the data, which makes it less useful if stolen but also reduces the accuracy of any computations performed on it.

TripleBlind’s Privophy technology addresses many of these issues, and indeed, TripleBlind argues that it complements confidential computing. As it says in a white paper on the subject: “When used alongside TripleBlind’s Blind Data Utilization Toolbox, secure enclaves contribute to establishing and maintaining compliance with strict data privacy regulations, including HIPAA, GDPR, and data residency laws.” It is also complementary to differential privacy, the vendor continues.

Company information

Background

TripleBlind was founded in 2019 by CEO Riddhiman Das and COO Greg Storm. Das was previously product architect at EyeVerify, an optical-recognition tech vendor acquired by China’s Ant Group (which includes cloud service provider Alibaba) in 2016. He then moved across to hold the same role at Zoloz, a company formed as a result of the combination of biometrics and authentication expertise from Ant Financial and EyeVerify, and after 2017 he became head of international technology investments for Ant, a position he held until leaving to form TripleBlind. Storm was previously director of research at EyeVerify and later at Zoloz, a biometric-authentication developer belonging to Ant.

TripleBlind has raised a total of $10m in venture funding, most recently announcing an $8.2m round from a group of investors led by Quiet Capital and Alumni Ventures Group.

Current position

TripleBlind started out with the mission of enabling data liquidity in the healthcare sector, but its technology has wider relevance. For instance, if an individual or a company has accounts with multiple banks, one of those banks could use the platform to access data across all the others for analysis without actually gaining visibility into any of that data.

Equally, TripleBlind enables data to be monetized as the raw material for training a statistical analysis routine or a neural network, for instance. The company even argues that, once encrypted using its technology, an organization's data could be licensed for use by any number of third parties for such training activities, given the technology's ability to tightly control the uses of the encrypted data once it has left the collector's infrastructure. As for the compute overhead for its use, the company says it is around 4% extra CPU cycles.

Tripleblind currently has about a dozen paying customers in the healthcare and financial services sectors. The charging mechanism for TripleBlind is an annual license, whose size is calculated based on two factors. First is the number of counterparties, that is, how many processors will be working on the collector's data. There are three tiers for this: for two counterparties, for three, and for six and over.

The second factor is the size of the data collector. A small startup with revenue in the sub-$10m range, for instance, would pay $1,000 a month, whereas a Tier 1 Wall St bank could be signing up to a fee of $450,000 a year.

Future plans

TripleBlind currently services the financial services and healthcare industries. As data privacy regulation emerges globally, the markets need to operate on data while observing increasing privacy requirements. TripleBlind expects to service customers in advertising and media, especially as popular browsers and regulation impede cross-site cookies.

Today, TripleBlind is usable only in Python and SQL. In the future, the vendor expects to develop support for other popular programming languages and tools such as the R statistical programming language.

Key facts

Table 1: Data sheet: TripleBlind

Product/Service name	TripleBlind	**Product classification**	Data privacy, data clean room
Version number	1.17	**Release date**	October 2020
Industries covered	Financial services, healthcare, marketing data, fintech, and lending and credit	**Geographies covered**	North America, South-Eastern Asia, Europe, Middle East
Relevant company sizes	Enterprise	**Licensing options**	Annual license, based on number of counterparties (two, three to five, or six and

			over) and size of the data collector
URL	https://tripleblind.ai/	**Routes to market**	Direct sales, partnerships, reseller agreements
Company headquarters	Kansas City, Missouri, US	**Number of employees**	10

Source: Omdia

Analyst comment

As discussed in **Product overview**, each of the proposed methods of achieving privacy for data that is shared with a third party for some form of computation has its advantages and shortcomings, and different tech groups advocate each:

- **Homomorphic encryption** tends to be quite slow and is very compute intensive. There are also academic debates about whether homomorphic encryption is quantum-resistant.
- **Confidential computing** does not address the issue of data anonymization and is hardware dependent.
- **Differential privacy,** like homomorphic encryption, cannot operate on audio or video files.

TripleBlind's Privophy technology addresses many of these issues, and indeed, TripleBlind argues that it complements confidential computing by contributing to the establishment and maintenance of compliance with strict data privacy regulations including HIPAA, GDPR, and data residency laws.

TripleBlind is, of course, a small startup without a lot of name recognition in the market as yet, and its tech offering must compete for attention with those of much larger vendors. Therefore, it will need to rely heavily on partnerships to raise its profile and to reach more potential customers.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

2021 Trends to Watch: Data Security (December 2020)

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com