



Conclave

A platform to securely share and analyze data ●



Data sharing across firms and departments is key to unlocking greater potential, analytics and insights. However, it remains one of the more difficult things organizations can do because of an inherent mistrust in how data is processed and used.

In today's digital climate, businesses demand more than a privacy policy or the promise of a firm's reputation to feel comfortable sending private data to a third party. Instead, they want to know exactly how their data is being used—all without giving up any control.

That's why R3 developed **Conclave**—a platform for developing applications that analyze and share private data from multiple parties—without compromising on confidentiality. Conclave takes data sharing to a whole new level. It is a platform that enables multiple parties to contribute data for analysis without revealing the actual data to anyone. Conclave is the ideal solution for software vendors, data service providers, exchanges, corporates and other firms looking to solve the data privacy challenge.

conclave

Build privacy protecting solutions with ease

Without inherent trust, there are limits to the types of solutions firms can build. There are also limits to their ability to enter new markets, pass along innovation and insight to their customers, and gain greater potential from existing data solutions.

Conclave opens several business use cases for software vendors to process previously inaccessible data and build high-value multi-party analytics. For example, they can now use Conclave to capitalize on:

- Fraud Detection
- Market Data Aggregation
- Private Order Matching
- Analytics Solutions

By leveraging cutting edge technologies such as Confidential Computing and Intel® SGX, the Conclave platform paves the way for a new generation of trusted and shared data services that unlock greater business value.



A survey conducted by Harris Poll shows that only 20% of US consumers “completely trust” the organizations they interact with to maintain the privacy of their data.

Fraud Detection

Challenges:

- Fraud that is spread across multiple institutions often remains undetected as there has been no way to securely pool multiple private data sets from industry participants to identify and prevent fraud.
- There are limits to the types of services that fraud detection software vendors can provide as there are data privacy regulations and concerns with sharing confidential customer data with a third party.

Solution: Conclave enables fraud detection software firms to access these private data sets by providing assurances to their customers that their data will not be viewed by the provider or the provider's other customers, just processed. As a result, these software firms can build new solutions that aggregate data from multiple firms in a trustworthy manner, while reducing false positives and detecting new fraud.

Market Data Aggregation

Challenge:

- Firms need to know how big their market is in order to calculate their own market share and forecasts, however, they do not feel comfortable sharing proprietary sales data such as new and recurring license revenue with a third-party provider.

Solution: Conclave enables firms to securely upload revenue and other proprietary sales data to a service that calculates relevant statistics, all without allowing the operator of the system to see the raw data, saving time and costly development resources.

Private Order Matching

Challenge:

- Traders often want to do price discovery and order matching privately, and also want to make sure that no one—not even the market operators—can misuse their private transaction details.

Solution: Conclave enables firms to build private order matching solutions that give assurances that private transaction data will not be viewed or misused. As a result, software firms can build solutions that protect market participants' data, giving traders and regulators confidence that they are trading in a fair and transparent marketplace.

Analytics Solutions

Challenge:

- Companies want to benefit from insights that Analytics and AI firms can provide, but do not feel comfortable sending confidential data outside of their organization, or having it pooled with their peers.

Solution: Conclave enables Analytics and AI firms to deliver solutions that provide transparency into how data is processed and assurances that customer data is protected. This enables end users to benefit from insights derived from analytics solutions without having to compromise on data privacy. Software firms can either build new solutions or develop on existing analytics solutions and run them across new private data sets.

Why Conclave?

With Conclave, independent software vendors (ISVs) and service providers can build trusted, shared data services that combine information from multiple parties to address new use cases and enable cross-company collaboration.

Figure 1 highlights the opportunity for ISVs to securely pool data from multiple customers and provide new solutions based off that pooled private data. Here we see clients first validating that they are talking to a 'secure enclave' that is running a specific algorithm that they have already decided they trust. Then, they upload their sensitive data to be pooled with that of other clients, safe in the knowledge that it will be processed only as agreed.

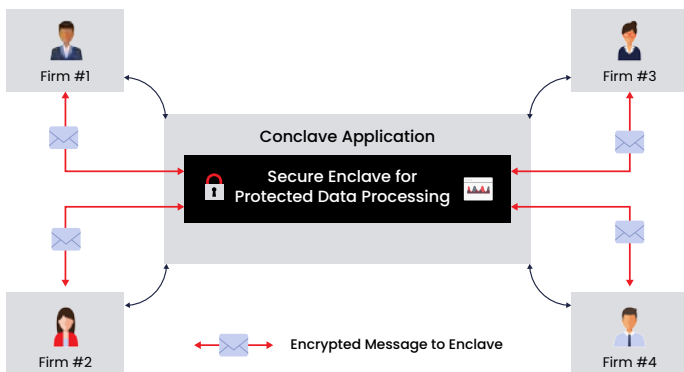


Figure 1: Multi-party data pooling

Confidential Computing

Conclave harnesses the capabilities of Confidential Computing and uses Intel® SGX, a Trusted Execution Environment that prevents the owner of a computer from influencing the enclave to do anything other than what it was written to do or seeing the data it is operating on.

Trusted Execution Environments (TEEs) allow programs to run inside secure enclaves which are isolated from the rest of the computer on which they run. TEEs ensure that data and code can be processed without the owner of the computer gaining access to the raw data. As a result, programs are resistant to physical and software attacks by the owner or operator of the computer, as well as by outside parties.

R3 joined the Linux Foundation's **Confidential Computing Consortium** in 2020 and is proud to sit alongside our peers as we work together to accelerate the acceptance and adoption of Confidential Computing in the marketplace.

Who can benefit from Conclave?

Conclave is for firms who want to build products and services that provide transparency into how data is collected and processed. The businesses who are end-users of Conclave-based applications also benefit as their data is protected from misuse and they are able to retain ownership and control of their data.

Conclave is also for software firms who are in the process of selecting a platform on which to build multi-party analytics. Firms can either build new solutions or develop on existing solutions and run them across new private data sets.

Which types of institutions can be transformed by building on Conclave?

- Financial Services firms
- Analytics firms and companies leveraging AI
- Data service providers
- Exchanges
- Fraud detection and compliance software firms
- Corporates
- Regulators

Key benefits of Conclave

- Process data from multiple parties to solve problems for a whole industry
- Protect customer data from misuse and provide assurance that the data remains protected when collected, shared and analyzed
- Reduce time-to-market for privacy-enhancing applications
- Access previously inaccessible customer data to deliver new insights and AI without sacrificing individual privacy
- Streamline business processes between firms, while sharing processing costs and infrastructure
- Increase effectiveness of Financial Crime detection by eliminating false positives
- Promote transparent and fair price discovery in Dark Pools

Key features of Conclave



Developer-friendly: A high-level, intuitive API brings the world of trusted execution to regular business developers who can write applications on any operating system (macOS, Linux, Windows)



Code in the language of your choice: Write confidential computing applications in Java, Kotlin and JavaScript, with new languages being added all the time



Focus on business logic: Conclave's innovative 'Mail' feature takes care of the messaging and persistence, allowing you to focus on the business logic. All the complexities of interacting with secure enclaves are abstracted behind an intuitive API



Compatible with Corda Enterprise: Conclave is available as stand-alone and is compatible with R3's flagship DLT platform Corda Enterprise

Get in touch

To download Conclave and start building today or for more information, visit www.conclave.net.

About R3

R3 is a leading provider of enterprise technology and services that enable direct, digital collaboration in regulated industries where trust is critical. Multi-party solutions developed on our platforms harness the "Power of 3"—R3's trust technology, connected networks and regulated markets expertise—to drive market innovation and improve processes in banking, capital markets, global trade and insurance.

As one of the first companies to deliver both a private, distributed ledger technology (DLT) application platform and confidential computing technology, R3 empowers institutions to realize the full potential of direct digital collaboration. We maintain one of the largest DLT production ecosystems in the world connecting over 400 institutions, including global systems integrators, cloud providers, technology firms, software vendors, corporates, regulators, and financial institutions from the public and private sectors.

Learn more at www.r3.com, www.conclave.net and www.corda.net.



Stay
connected
with R3

 @inside_r3

New York

1155 Avenue of the Americas,
34th Floor
New York, NY 10036

London

2 London Wall Place,
London, EC2Y 5AU

Singapore

18 Robinson Road,
Level 14-02
Singapore, 048547

São Paulo

Av. Angélica, 2529 - Bela Vista
6th Floor
São Paulo - SP, 01227-200, Brazil