Fraud Analysis

Secure and fraud-free transactions.

VU

Datasheet

Version 5.28.0

April 2024

What is?

Fraud Analysis is a multi-channel fraud prevention solution that gives organizations' fraud analysts the ability to create user profiles and identify potentially fraudulent transactions that deviate from established patterns.

This tool analyzes user behavior across multiple channels, allowing for proactive detection and prevention of fraud and identity theft attempts.

By triggering alerts when transactions deviate from normal patterns, **Fraud Analysis** enables real-time adjustments to fraud detection rules, keeping up with evolving attack methods.

Furthermore, through forensic analysis, it facilitates the investigation and reconstruction of suspicious transactions and events. This empowers fraud analysts to gather evidence, take appropriate actions based on findings, and configure new rules to prevent future occurrences.

Benefits

• Establishes transaction rules to proactively classify them based on their risk potential, enhancing fraud prevention measures.

• Collects information from multiple channels in a user-friendly way, eliminating the need for technical expertise in administration.

• Utilizes a wide range of customizable variables to define fraudulent events or transactions, ensuring flexibility in identifying fraud patterns.

• Generates real-time complex event processing (CEP) rules to promptly detect and respond to attacks.

• Evaluates secure zones for each user by considering their transaction history, schedules, and device geolocation, adapting to individual user patterns.

• Generates dynamic reports by channels, users, specific rules, and generated analyses, providing comprehensive reporting capabilities.

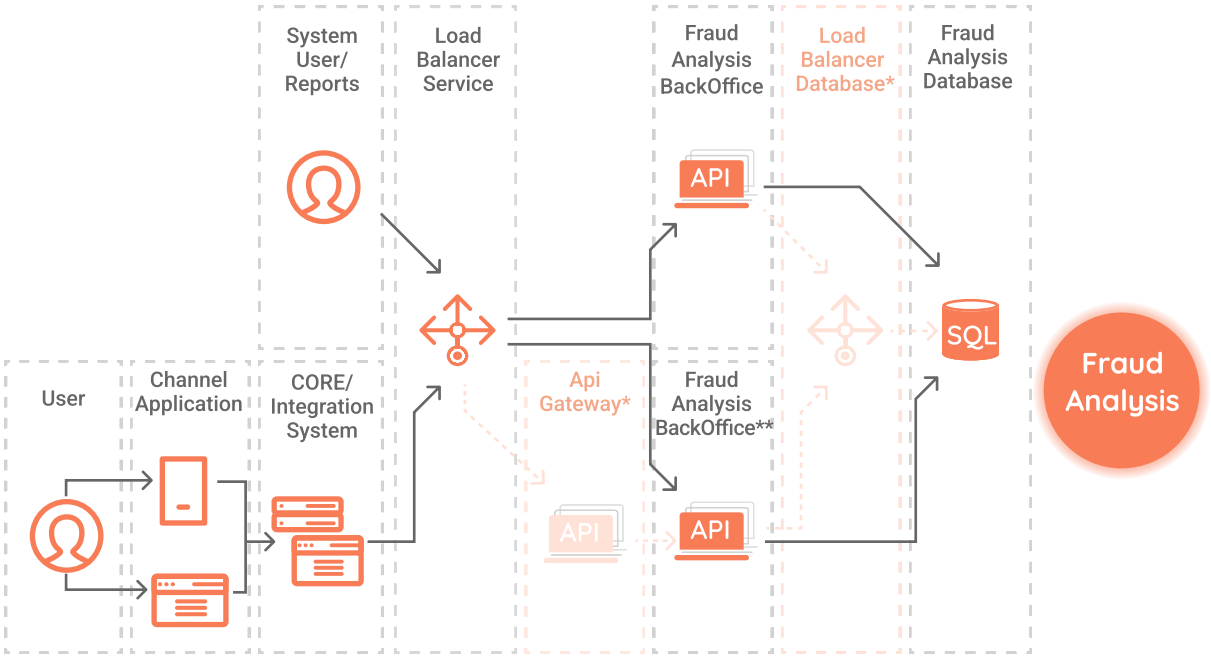
• Presents data in various real-time formats, including grids, tables, and graphs, and enables data extraction in CSV, PDF, and XLSX formats for easy analysis.

Outstanding use cases

- Financial technology (fintech) and digital banking.
- E-commerce platforms and online stores.
- Financial companies and stock exchanges.
- Customer rewards and loyalty programs.
- Prevention of money laundering from transactions originating from illegal or unregulated sources.

Operating logic diagram

Fraud Analysis can be purchased as a cloud service, on-premises software licensing, or a hybrid solution.



** Optional*

*** CEP requires a license to work with more than one node*

Focus on user experience

At **VU Security**, we understand the importance of user experience in cybersecurity solutions. Tools should be built with users' everyday lives in mind, helping them understand, use, and benefit from the product.
In response to this need, we have designed a user-centric solution that makes it easy for fraud analysts to identify suspicious transactions and visualize risk alerts.

Fraud Analysis Backoffice

Fraud Analysis provides all the necessary methods to analyze all types of transactions or events:

User scoring
Assigns risk scores based on typical user behavior.

Rules engine
Executes actions in real time based on predefined and customizable rules.

Classifiers
Combines existing conditions and rules, streamlining the system's response.

Occurrence counter
Counts the number of occurrences of certain variables over a specified period of time.

Case Management
Manages cases and tracks potential fraud attempts in customizable dashboards.

Risk-based authentication
Defines the level of authentication required based on the risk levels of frequent events.

Multi-node support
Multiple instances or nodes can query the same database without overlap.

Reports and Analytics
Generates predefined and customizable reports.

Bulk loading (historical)
Allows bulk loading of transactions and events from the same date or earlier in .csv files.

Forensic Analysis
Evidence collection with the possibility of attaching all necessary documentation to resolve cases.

Deny and allow lists
Creation of lists that specify which devices are prohibited or allowed based on specific criteria, patterns, or characteristics.

Integration API

The solution's infrastructure is designed to integrate with any other platform, regardless of the language used, through REST API services. Communication between the server and the application is done through an SSL/TLS connection.

The methods that make up the solution are designed for the administration of the end users. They allow to:

- Alert and block suspicious transactions.
- Configure rules to define fraudulent transactions and events.
- Generate dynamic reports by channels, users, and rules.
- Recognize user's typical behavior with Predictive Models.
- Download information in .CSV and/or PDF, XLSX file formats.

It is carried out using REST methods, always using a secure SSL channel (port 443).

Technical information

Hardware and software requirements

Fraud Analysis has a framework with extensive integration capabilities with different systems, such as Microsoft and Cisco, among others.
It allows the creation of predictive models to optimize the process, analyze different types of events and reduce transactional fraud.

Database	App Server	Java	Devices compatibility (SDK)
MS SQL 2017 or higher (*)(**)	Tomcat 9.0.54 or the lower version available (*)	Java JRE 11	iOS 11 or higher
Oracle 18.0 or higher			Android 5 or higher
PostgreSQL v13 or higher			

(*) Recommended

(**) Supplied in the installation packages.

Hardware sizing

Monolithic Rules Engine

For versions lower than 3.6.7 the model has three layers:

- Database
- Application layer (API Server)
- Administration layer (Backoffice + reporting)

Users	TPS	CORES	RAM	System Storage	DB Storage
250.000	8	2	4	60 GB	20 GB
500.000	16	4	8	80 GB	40 GB
1.000.000	32	8	16	100 GB	80 GB
2.000.000	64	16	32	120 GB	160 GB
> to 2.000.000	Consult us	Consult us	Consult us	Consult us	Consult us

Modularized Rules Engine (it does not include CEP)

The following sizing is based on the new Fraud Analysis architecture in which the CEP rule engine has been modularized.

TPS	WEB CPU	WEB RAM	DB CPU	DB RAM
100	4 cores	8 GB	2 cores	8 GB
250	4 cores	8 GB	4 cores	8 GB
400	4 cores	8 GB	8 cores	16 GB
600	8 cores	16 GB	8 cores	16 GB
900	8 cores	16 GB	16 cores	16 GB

Support

Support level

VU Security will provide **level 3 support**.

Support includes a set of technologies and rights to help the customer maximize the investment made in VU Security licenses.

To contact VU Security support team, please send an email to: customer.support@vusecurity.com

As soon as your email is received, you will be automatically assigned a case and you will receive all the news related to your case in the same email thread.

If you want to add recipients, put them on a copy. Put Subject: [Name of the client] [Criticality] [Title of the problem].

Support cases are dealt with from **Monday to Friday from 9 a.m. to 6 p.m.** (Argentina).

Contactos

Otros productos de VU Security

Our solutions offer a 360° experience, each contributing an essential aspect to the security strategy of both users and organizations.

Onboarding Management:
• ID+Face
• Voice
• Touch

Authentication Management:
- Server
- SDK
- App

CIAM / IAM

If you need more information or want to schedule a demo of this solution, please write to us at: sales@vusecurity.com

About VU Security

VU is a global cybersecurity company specializing in identity protection and fraud prevention. We develop modular, easy-to-integrate solutions that are adaptable for both corporate and government sectors.

To achieve this, we utilize innovative technologies that combine traditional cybersecurity controls with biometrics, geolocation, artificial intelligence, predictive models, document recognition, and user behavior analysis.

More than 350 million people worldwide and over 130 clients in 30 countries across Latin America, Europe, and the United States rely on VU Security's technology to digitize their businesses and enhance operational efficiency while reducing the risks of attacks and information loss.

Our strategic alliances with Microsoft, Telefónica, IBM, BGH, Intel, Cisco, Accenture, and other companies contribute to VU Security's mission: to create secure and frictionless experiences that improve the quality of life for individuals and organizations.

vusecurity.com