VU

Fraud Analysis

Secure transactions without fraud.

Datasheet

V 3.0.68

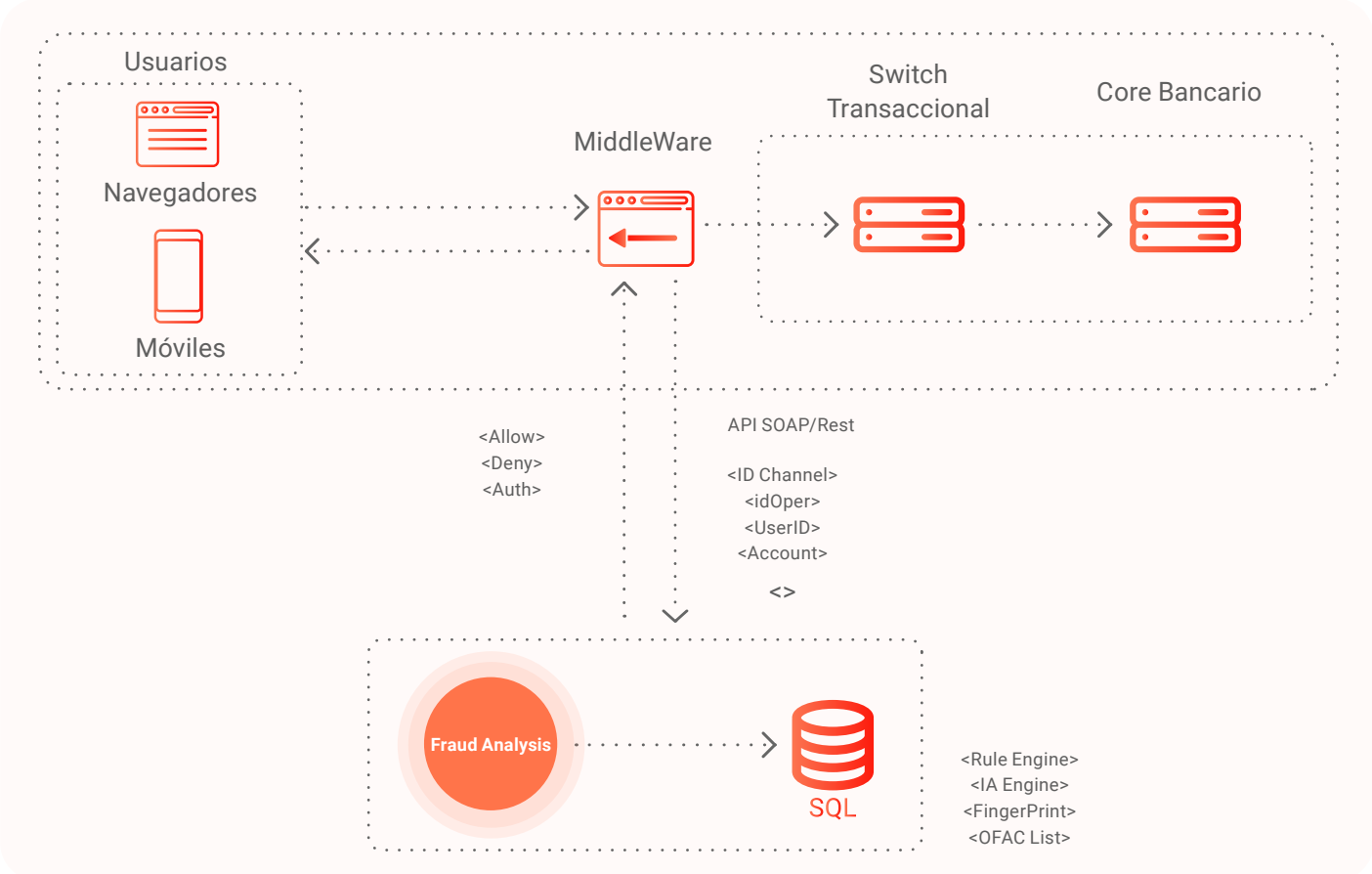
What is Fraud Analysis?

By means of artificial intelligence and an unerring combination of solutions adapted to the business, both the digital identity of users and the company's IT resources are safeguarded. When customers feel that their information is protected, they feel comfortable to operate and use the services provided by the company on a regular basis. How Fraud Detection works: both users' behavior and the channels through which they operate are analyzed in order to prevent possible fraud and identity theft promptly. Thus, by means of AI, the system warns of and blocks transactions that may pose a threat to the business.

Thanks to the use of machine learning, the solutions identify, report and respond to threats to the security of platforms, systems and applications. In this way, monetary loss and reputation damage are avoided.

VU Fraud Analysis includes an online reporting module that enables the creation of dynamic reports by channels, users, specific rules, generated analysis, etc. It provides a variety of models and data that support real-time reporting through grids and graphs. In addition, it enables exporting the information to editable files such as .CSV and/or PDF, XLSX and also processing the information in a customizable way.

Diagrama lógico de funcionamiento



Integration

- Banks
- Fintech companies
- Finance companies
- Stock brokerage companies

Focus on user experience

We know that user experience is important in this type of solutions as it has an impact on the business, and security must be provided accordingly. Therefore, our product is designed and tested with users frequently, thus understanding and measuring their experience in order to maximize it.

System and software requirements and compatibility

VU provides a framework with broad capabilities to integrate with different systems, including Microsoft and Cisco, among others. It operates using business intelligence, machine learning and Microsoft Cognitive Services technology to optimize the onboarding process and reduce fraud.

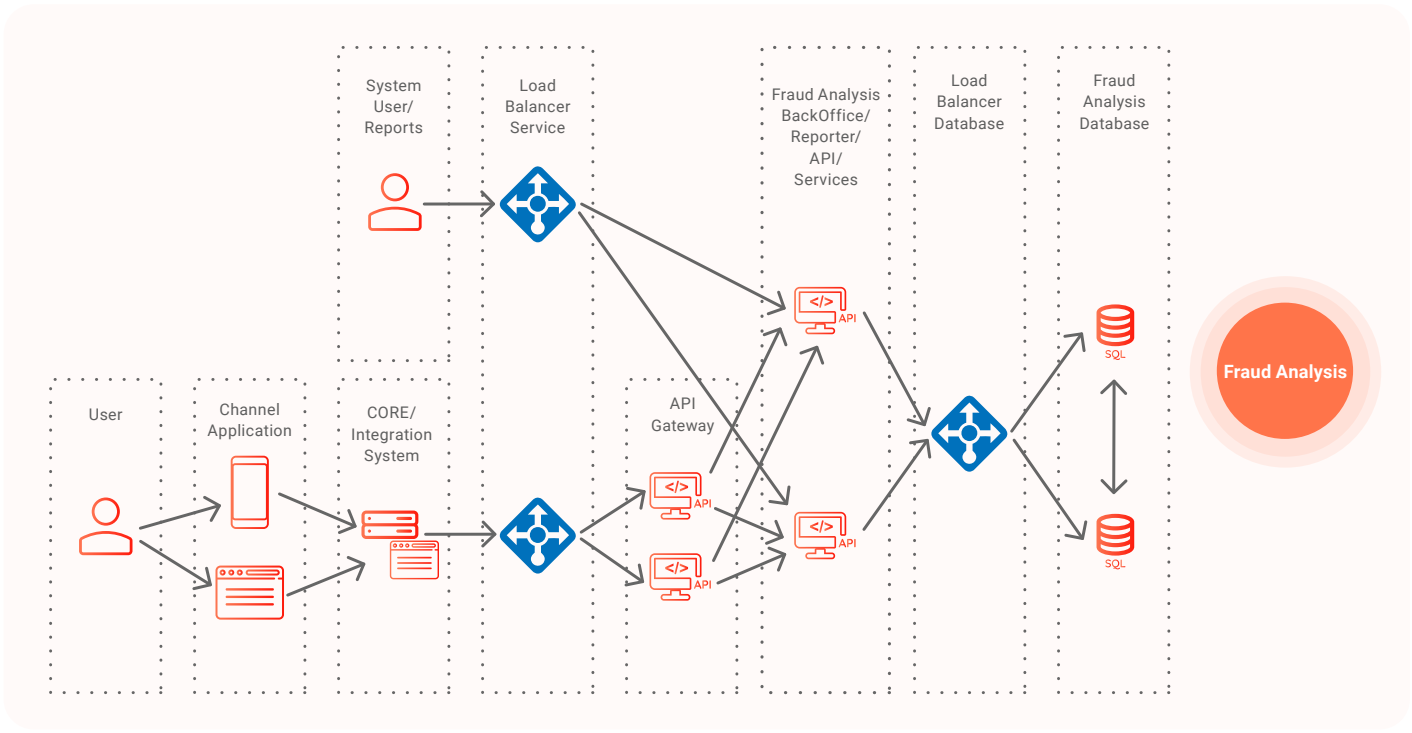
Operating System	Database	App Server	Java
Centos/Redhat 7.9 (*)	**PostgreSQL 9 or higher (*)**	**Tomcat 9.31 or higher (*)**	**1.8**
Ubuntu LTS (*)	**MS SQL 2019 or higher**	**Jboss 7.11 or higher**	
Windows Server 2019			

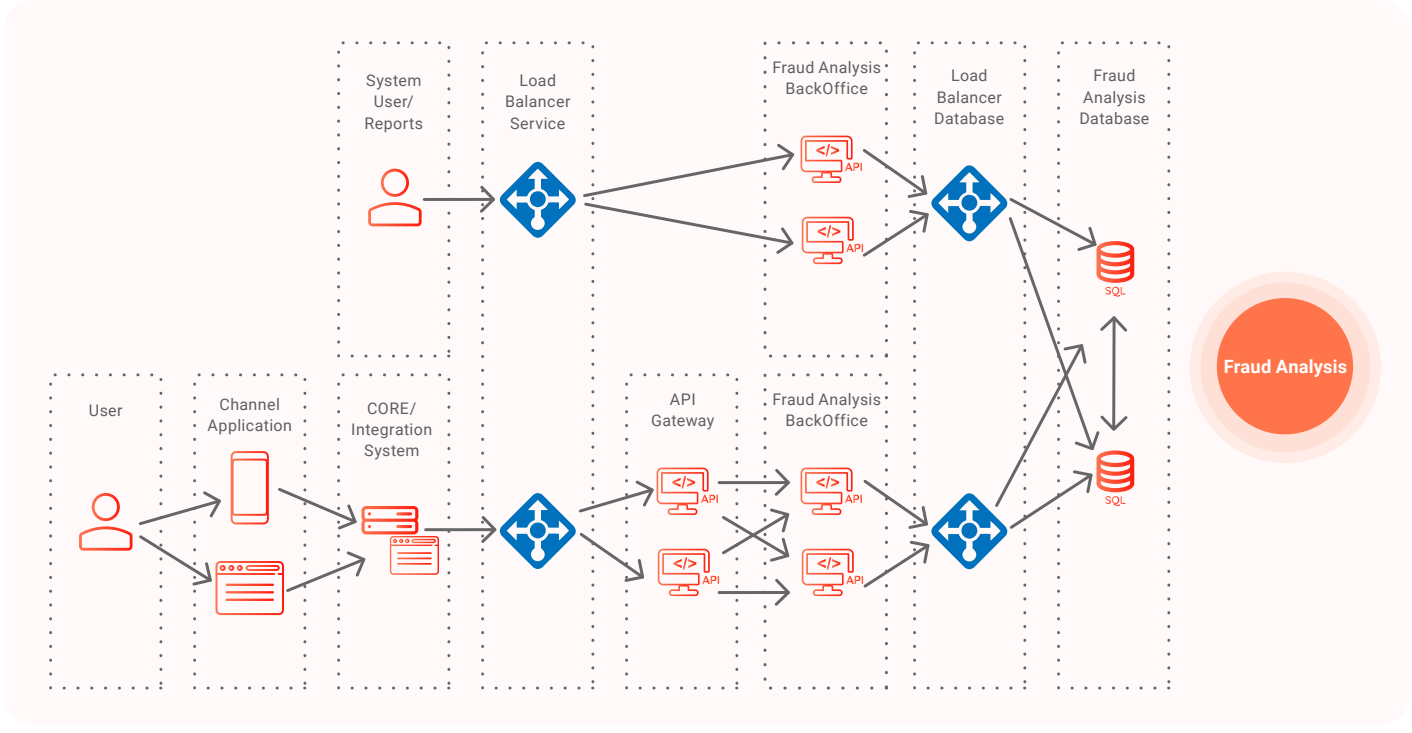
*Recomendado

Architecture & Environment Diagram

The solution can operate in the following environments:

- Cloud
- On premise
- Hybrid





Hardware Sizing

3-layer model of Fraud Services (API Server) or 2-layer model of Fraud Server (API Server + Backoffice)

FRAUD

Users	TPS	CORES	RAM	System Storage	Month DB Storage ***	Annual DB Storage
250,000	8	2	4	60 GB RAM	20 GB	240 GB
500,000	16	4	8	120 GB RAM	40 GB	480 GB
1,000,000	32	8	16	240 GB RAM	80 GB	1.2 TB
2,000,000	64	16	32	480 GB RAM	160 GB	2 TB
2.000.000 or more	**Ask your BSA**					

3-layer model Fraud Backoffice

FRAUD

		Minimal			Recomended		
Users	TPS	CORES	RAM	System Storage	CORES	RAM	System Storage
250,000	8	2	4	60 GB	8	16	240 GB
500,000	16	4	8	120 GB	16	32	480 GB
1,000,000	32	8	16	240 GB	32	64	960 GB
2,000,000	64	16	32	480 GB	64	128	2 TB
2.000.000 or more	**Ask your BSA**						

Noteworthy use cases

- One-click online Check-out.
- Users scoring.
- Money laundering prevention.
- Mule account detection.

Additional VU products that enhance VUTM Fraud Analysis

- VUTM Face Recogn
- VUTM Voice Recogn
- VUTM Sign
- VUTM Application Server
- Secure Onboarding Process

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