Fraud Analysis

Transacciones seguras sin fraude.

Datasheet

V 3.0.68

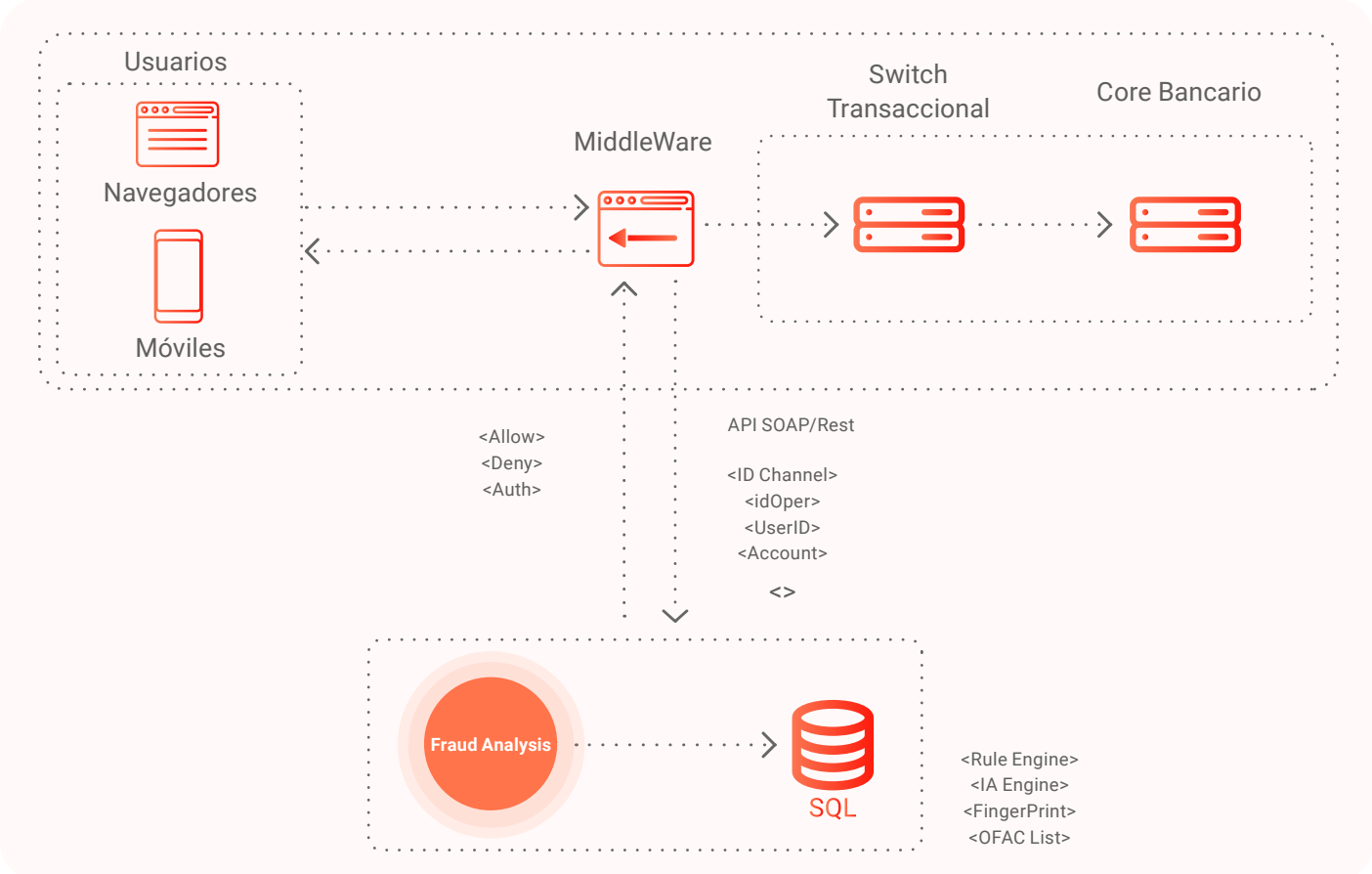
¿Qué es?

Mediante inteligencia artificial y una combinación infalible de soluciones adaptadas al negocio, tanto la identidad digital de los usuarios como los recursos informáticos de la compañía quedan resguardados. Cuando un cliente considera que su información está protegida, se siente cómodo para operar y utilizar los servicios de la empresa con frecuencia. Cómo funciona Detección de fraude, se analiza el comportamiento de los usuarios y canales en los que operan para detener a tiempo posibles fraudes y robo de identidad.
De esta manera, utilizando IA el sistema alerta y bloquea transacciones que pueden ser una amenaza al negocio.

Gracias a la utilización de machine learning, las soluciones detectan, informan y actúan frente a los peligros que amenazan la seguridad de plataformas, sistemas y aplicaciones. De esta forma, se evitan pérdidas monetarias y daños a la reputación.

VU Fraud Analysis cuenta con un módulo de reportes en línea que permite extraer reportes dinámicos por canales, usuarios, reglas específicas, análisis generados, etc. Cuenta con diversos modelos y datos que permiten emitir reportes en grillas y gráficos en tiempo real. Además, permite exporta la información a archivos modificables como .CSV y/o PDF, XLSX y poder tratar la información de manera personalizada.

Diagrama lógico de funcionamiento



Integraciones

- Bancos
- Fintech
- Compañías Financieras
- Validar el fingerprint de un usuario.
- Sociedades de Bolsa

Foco en Experiencia de Usuario

Sabemos que es importante la experiencia del usuario en este tipo de soluciones. Lo sabemos porque entendemos que la experiencia del usuario afecta al negocio y la seguridad debe proveerse en función de eso. Es por eso por lo que diseñamos y probamos con usuarios nuestro producto frecuentemente, entendiendo y midiendo la experiencia para poder maximizarla.

Requisitos y Compatibilidad de Software

VU cuenta con un framework con amplias capacidades para integrarse con diferentes sistemas, incluyendo Microso¬ y Cisco, entre otros. Trabaja con tecnología de business intelligence, machine learning y Microso¬ Cognitive Services para optimizar el proceso de onboarding y reducir el fraude

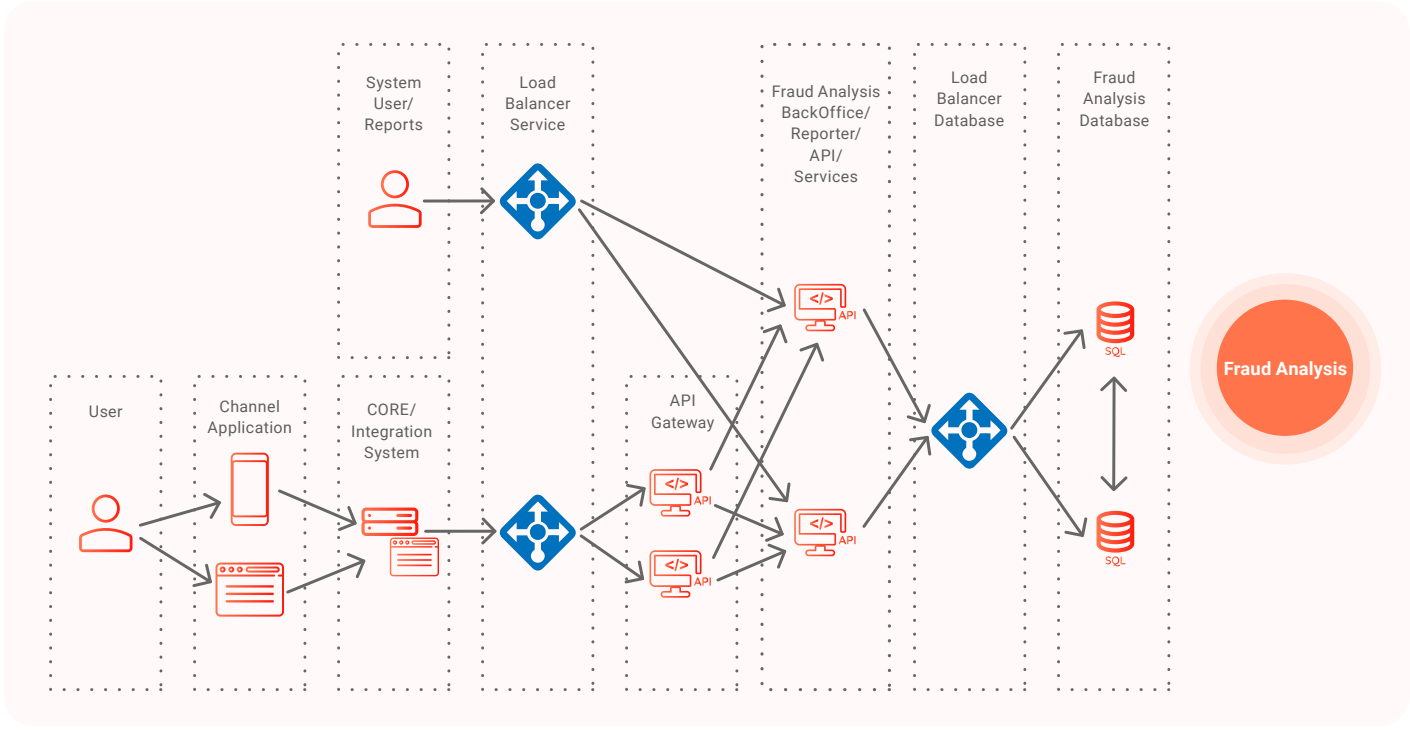
Sistema Operativo	Base de Datos	App Server	Java
Centos/Redhat 7.9 (*)	**PostgreSQL 9 o superior (*)**	**Tomcat 9.31 o superior (*)**	**1.8**
Ubuntu LTS (*)	**MS SQL 2019 o superior**	**Jboss 7.11 o superior**	
Windows Server 2019			

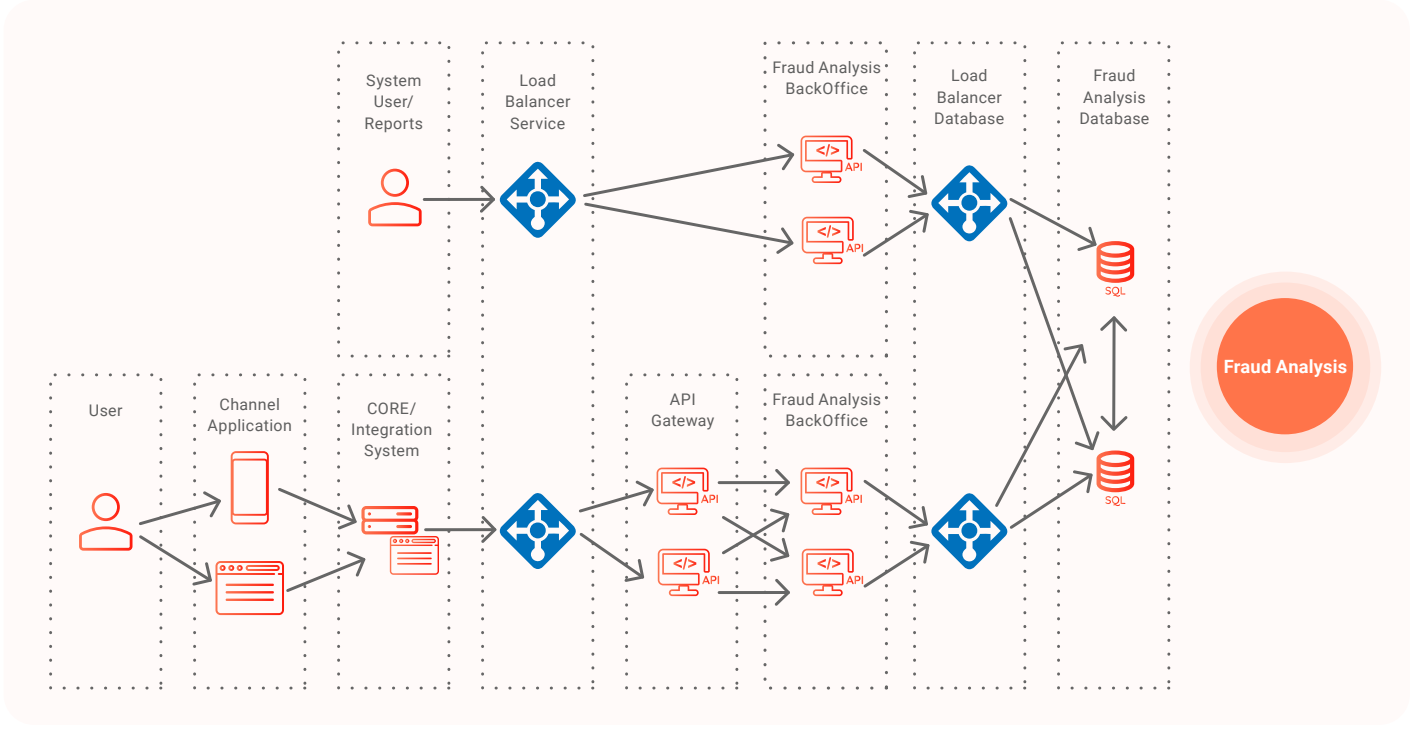
*Recomendado

Diagrama de arquitectura & Ambientes

La solución puede trabajar en los siguientes ambientes:

- Nube
- Onpremise
- Hibrido





Dimensionamiento de hardware

Fraud Services (API Server) en modelo de 3 capas o Fraud Server (API Server + Backoffice) en modelo de 2 capas

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**					

Fraud Backoffice en modelo de 3 capas

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**						

Casos de uso destacados

- Online Check-out en unclick.
- Scoring de usuarios.
- Prevención de lavado de dinero.
- Detección de cuentas mula.

Otros productos de VU que potencian Fraud Analysis®

- VU Face Recogn®
- VU Voice Recogn®
- VU Sign®
- VU Application Server®
- Secure Onboarding Process®

Si necesitas más información o quieres agendar demo de esta solución, por favor escríbenos a: sales@vusecurity.com