Fraud Analysis

Transacciones seguras sin fraude.

Datasheet

V 3.0.68

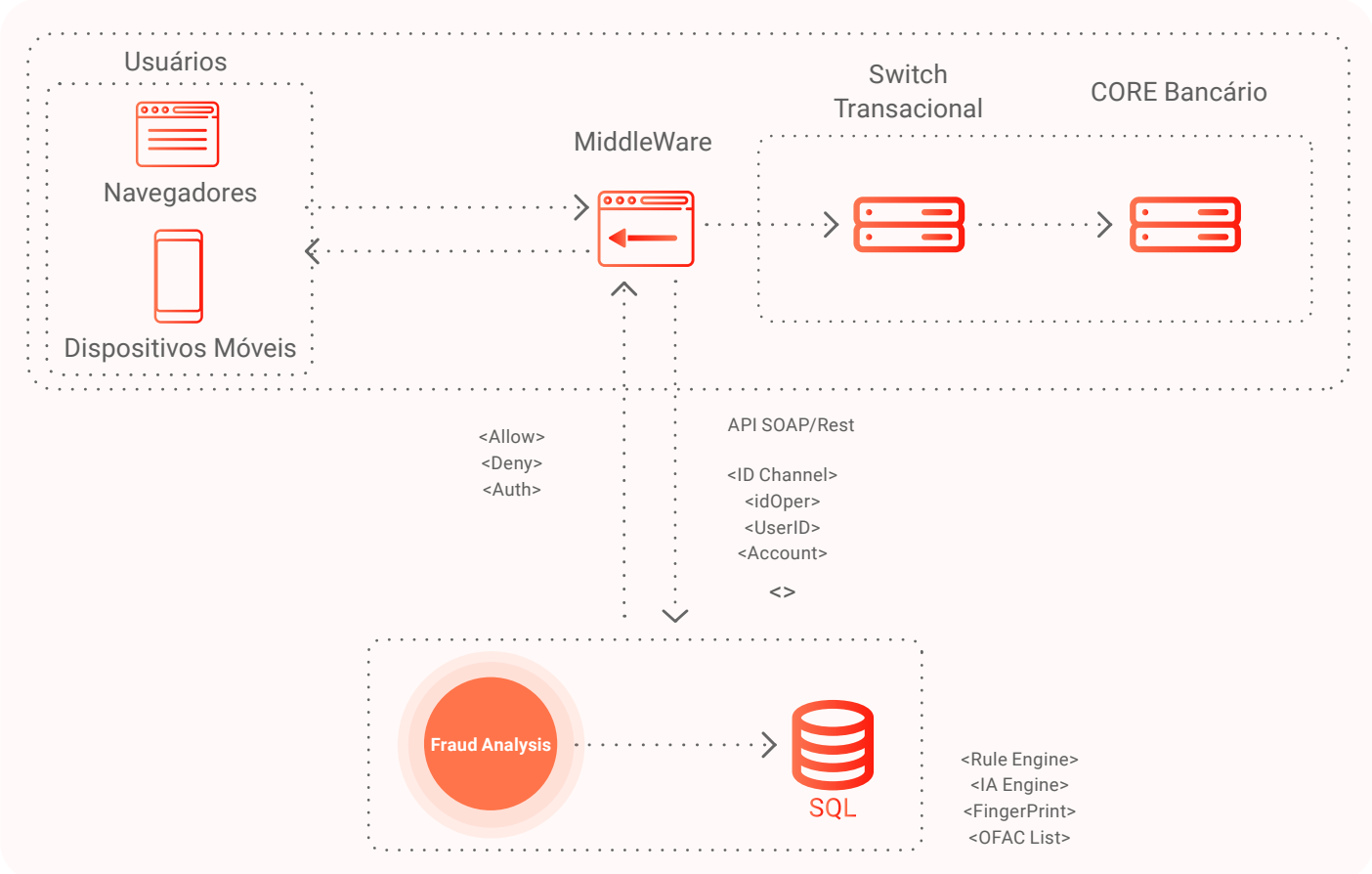
O que é VU Fraud Analysis®?

Por meio de inteligência artificial (IA) e uma combinação infalível de soluções adaptadas ao negócio, tanto a identidade digital dos usuários quanto os recursos computacionais da empresa ficam protegidos. Quando um cliente confia que suas informações estão protegidas, ele se sente confortável para operar e usar os serviços da empresa normalmente. Como funciona a Detecção de Fraudes: o comportamento dos usuários e os canais em que operam são analisados para impedir possíveis fraudes e roubo de identidade a tempo. Desta forma, através de IA, o sistema alerta e bloqueia transações que podem ameaçar o negócio.

Graças ao uso de machine learning, as soluções detectam, informam e agem contra os perigos que ameaçam a segurança de plataformas, sistemas e aplicações, desta forma evitando-se perdas financeiras e danos à reputação.

VU Fraud Analysis possui um módulo de relatórios online que permite extrair relatórios dinâmicos por canais, usuários, regras específicas, análises geradas, entre outros. Possui vários modelos e dados que permitem gerar relatórios em grades e gráficos em tempo real. Além disso, permite exportar as informações para arquivos editáveis, como CSV e/ou PDF, XLSX, de modo que as informações possam ser tratadas de forma personalizada.

Diagrama lógico de funcionamento



Integrações

- Bancos
- Fintech
- Instituições Financeiras
- Validação da impressão digital do usuário
- Corretoras de Bolsa de Valores

Foco na experiência do usuário

Sabemos que a experiência do usuário é importante neste tipo de solução porque entendemos que esta afeta diretamente o negócio, e a segurança deve ser fornecida com base nisto. É por isso que projetamos e testamos nosso produto com participação dos usuários frequentemente, entendendo e medindo sua experiência de forma a torná-la sempre melhor.

Integração

A VU possui um framework com grande capacidade de se integrar a diferentes sistemas, incluindo Microsoft e Cisco, entre outros. Trabalha com tecnologia de business intelligence, machine learning e Microsoft Cognitive Services para otimizar o processo de onboarding e reduzir fraudes.

Requisitos de Software e Compatibilidade

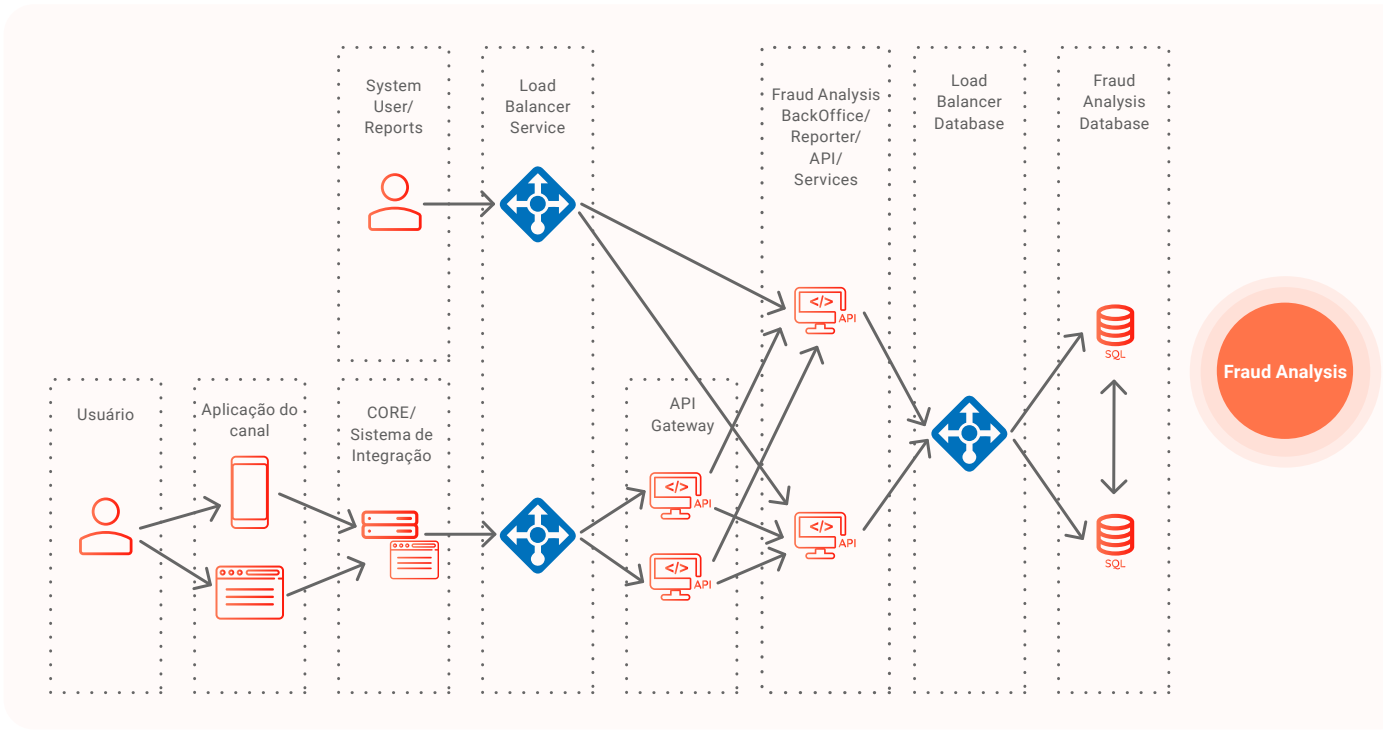
Sistema Operacional	Banco de dados	App Server	Java
Centos/Redhat 7.9 (*)	**PostgreSQL 9 ou superior (*)**	**Tomcat 9.31 ou superior (*)**	**1.8**
Ubuntu LTS (*)	**MS SQL 2019 ou superior**	**Jboss 7.11 ou superior**	
Windows Server 2019			

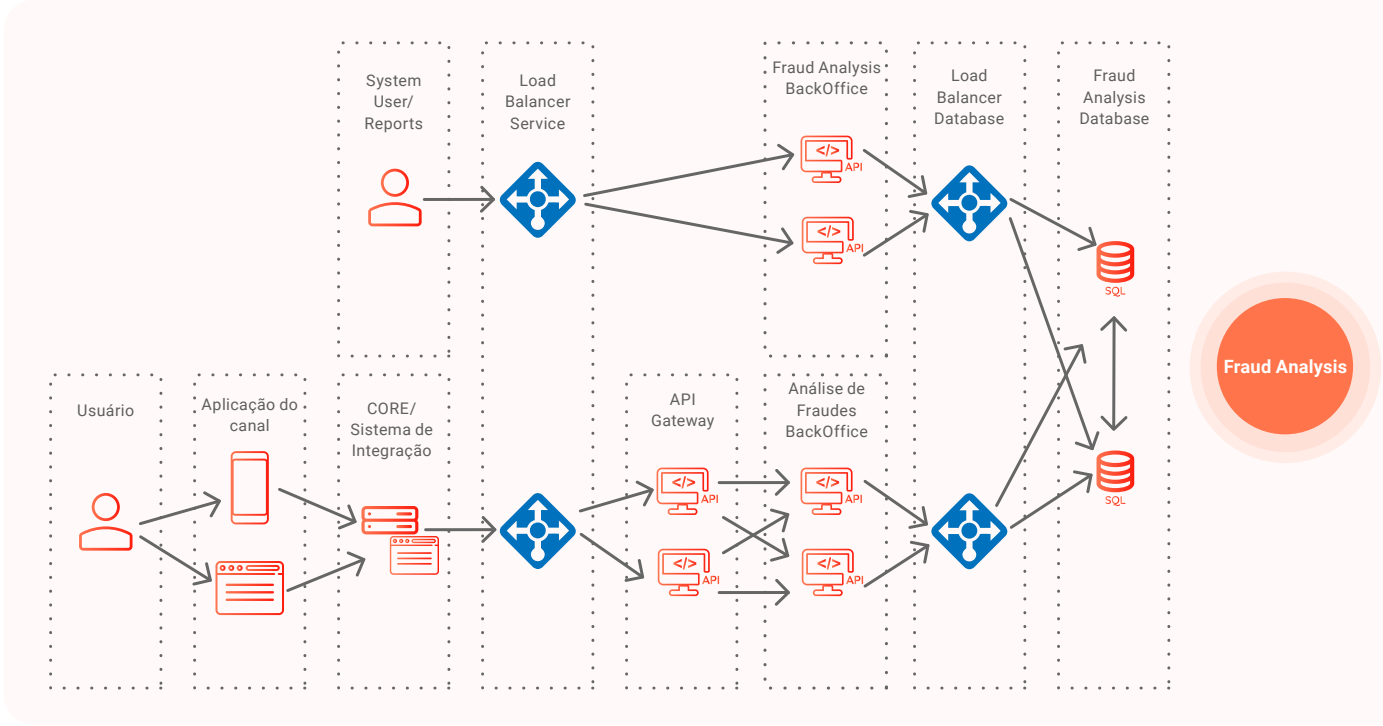
*Recomendado

Diagrama de Arquitetura & Ambientes

A solução pode funcionar nos seguintes ambientes:

- Nuvem
- Local
- Híbrido





Dimensionamento de hardware

Fraud Services (API Server) em modelo de 3 camadas ou Fraud Server (API Server + Backoffice) em modelo de 2 camadas

FRAUDE

Usuários	TPS	NÚCLEOS	RAM	Armazenamen-to do sistema	Armazenamento DB mensal ***	Armazenamento DB anual
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 ou acima	**Verifique com seu BSA**					

Fraud Backoffice em modelo de 3 camadas

FRAUD

		Minimal			Recomended		
Usuários	TPS	NÚCLEOS	RAM	Armazenamen-to do sistema	CORES	RAM	Armazenamento do sistema
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 ou acima	**Verifique com seu BSA**						

Casos de uso em destaque

- Check-out online em um clique.
- Pontuação (scoring) do usuário.
- Prevenção à lavagem de dinheiro
- Detecção de contas de laranjas.

Outros produtos VU que potencializam VU Fraud Analysis®

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

Se precisa de mais informações ou deseja agendar uma demonstração desta solução, por favor nos contate em sales@vusecurity.com