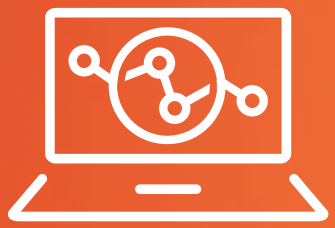


Fraud Analysis

Transacciones seguras y sin fraude.

Datasheet

Versión 5.28.0

Abril 2024

2024 VU Inc. Todos los derechos reservados.

¿Qué es?

Fraud Analysis es una solución de prevención de fraude multicanal que permite a los analistas de fraude de una empresa crear perfiles y detectar operaciones potencialmente fraudulentas cuando una transacción se sale de los parámetros habituales.

Esta herramienta analiza el comportamiento de los usuarios y los canales en los que operan, con el fin de alertar y detener a tiempo posibles casos de fraude y suplantación de identidad.

Fraud Analysis alerta cuando una transacción se desvía de los parámetros habituales y permite modificar en tiempo real las reglas de detección de fraude para adaptarse a la velocidad con la que se producen los ataques.

Además, a través del análisis forense, facilita la investigación y reconstrucción de transacciones y eventos sospechosos. De este modo, el analista de fraude puede recopilar evidencias, determinar las acciones a seguir según las conclusiones obtenidas y configurar nuevas reglas para prevenir futuros casos.

Beneficios

• Configura reglas sobre las transacciones para clasificarlas según su potencial de riesgo.

• Recibe información de distintos canales y no requiere conocimiento técnico para su administración.

• Contiene múltiples variables parametrizables que permiten definir qué tipo de eventos o transacciones serán consideradas como fraude.

• Capaz de generar reglas de procesamiento de eventos complejos (CEP) para la detección de ataques en tiempo real.

• Evalúa zonas seguras para cada usuario según su historial, horarios de transacciones y la geolocalización del dispositivo.

• Permite extraer reportes dinámicos por canales, usuarios, reglas específicas, análisis generados, etc.

• Dispone de diferentes modelos de datos en tiempo real como cuadrículas, tablas y gráficos, permitiendo extraer la información en archivos .CSV y/o PDF, XLSX.

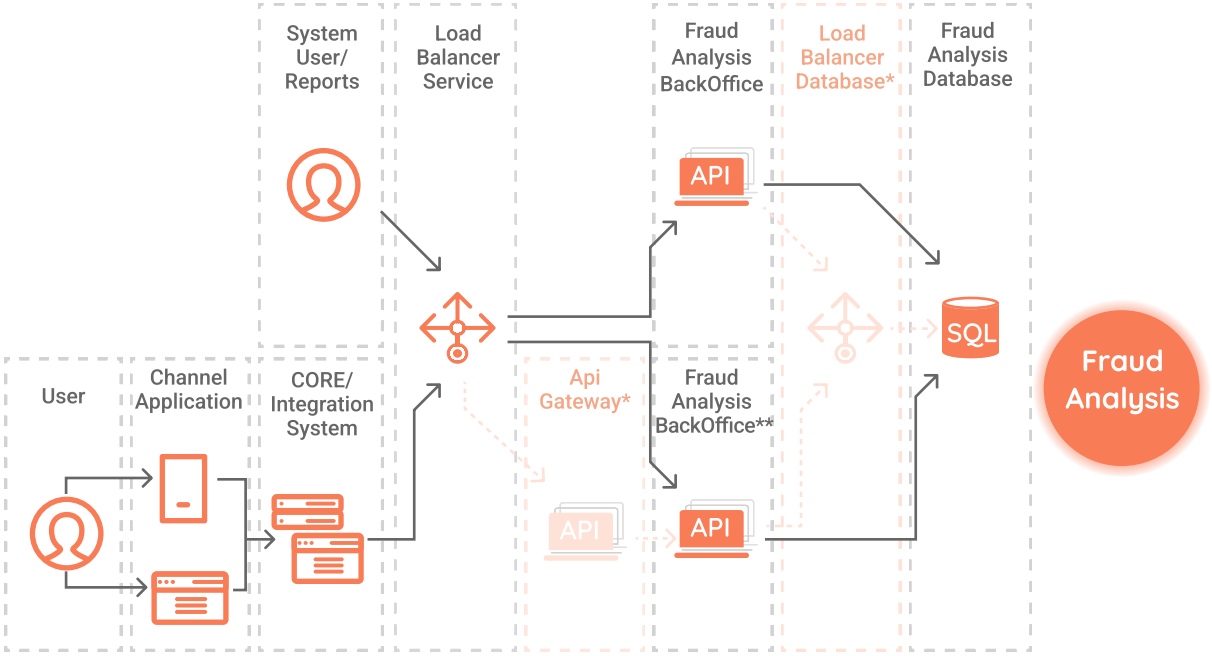
Algunos casos de uso más destacado

- Fintech y bancas digitales.
- Plataformas de e-commerce y tiendas virtuales.
- Compañías financieras y sociedades de Bolsa.
- Bonificaciones y programas de fidelización de clientes.
- Prevención del lavado de dinero de transacciones originadas por fuentes ilegales o no reguladas.

2024 VU Inc. Todos los derechos reservados.

Diagrama lógico de funcionamiento

Fraud Analysis se puede adquirir como servicio en la nube o como licenciamiento de software (on-premises) o híbrido.



** Opcional.*

*** CEP requiere licencia para trabajar con más de un nodo.*

Foco en la experiencia del usuario

En **VU Security** entendemos la importancia de la experiencia del usuario en las soluciones de ciberseguridad. Las herramientas deben construirse teniendo en cuenta la vida cotidiana de los usuarios para ayudarles a entender, utilizar y beneficiarse del producto.
En respuesta a esta necesidad, hemos diseñado una solución centrada en el comportamiento del usuario que facilita a los analistas de fraude la identificación de transacciones sospechosas y la visualización de alertas de riesgo.

2024 VU Inc. Todos los derechos reservados.

Backoffice de Fraud Analysis

Fraud Analysis cuenta con todos los métodos necesarios para analizar todo tipo de transacciones o eventos:

User scoring
Asigna puntajes de riesgo basados en el comportamiento habitual del usuario.

Motor de reglas
Ejecuta acciones en tiempo real a partir de reglas predefinidas y personalizables.

Clasificadores
Combina condiciones y reglas preexistentes, agilizando la respuesta del sistema.

Contabilizador de ocurrencias
Cuenta el número de ocurrencias de determinadas variables en un período de tiempo determinado.

Case Management
Gestiona los casos y hace seguimiento de los posibles intentos de fraude en tableros personalizables.

Autenticación basada en riesgo
Define el nivel de autenticación requerido en función de los niveles de riesgo de los eventos frecuentes.

Soporte para múltiples nodos
Es posible que múltiples instancias o nodos consulten la misma base de datos sin que se superpongan.

Reportes y Analytics
Genera reportes predefinidos y personalizables.

Carga masiva (histórico)
Permite la carga masiva en archivos .csv de transacciones y eventos de la misma fecha o anteriores.

Análisis Forense
Recopilación de pruebas con la posibilidad de adjuntar toda la documentación necesaria para resolver los casos.

Listas de rechazo y aceptación
Creación de listas que especifican qué dispositivos están prohibidos o permitidos a partir de criterios, patrones o características específicas.

2024 VU Inc. Todos los derechos reservados.

API de integración

La infraestructura está diseñada para integrarse con cualquier otra plataforma, independientemente del lenguaje utilizado, a través de servicios API REST. La comunicación entre dicho servidor y la aplicación se realiza a través de una conexión SSL/TLS.

Los métodos que constituyen la solución están diseñados para la gestión administrativa de los usuarios finales. Estos permiten:

- Alertar y bloquear transacciones sospechosas.
- Configurar reglas para definir las transacciones y eventos fraudulentos.
- Extraer reportes dinámicos por canales, usuarios y reglas.
- Reconocer el comportamiento habitual del usuario con modelos predictivos.
- Descargar la información en archivos .CSV y/o PDF, XLSX.

Se realiza mediante métodos REST, siempre utilizando un canal seguro SSL (puerto 443).

2024 VU Inc. Todos los derechos reservados.

Información técnica

Requisitos y compatibilidad de software

Fraud Analysis tiene un marco con amplias capacidades para integrarse con diferentes sistemas, incluidos Microsoft y Cisco, entre otros.
Permite crear modelos predictivos para optimizar el proceso, analizar distintos tipos de eventos y reducir el fraude transaccional.

Base de datos	App Server	Java	Compatibilidad dispositivos (SDK)
MS SQL 2017 o superior (*)(**) Oracle 18.0 o superior PostgreSQL v13 o superior	Tomcat 9.0.54 o la versión inferior disponible	Java JRE 11	iOS 11 o superior Android 5 o superior

(*) Recomendado
(**) Se recomienda utilizar versiones LTS

2024 VU Inc. Todos los derechos reservados..

Dimensionamiento de hardware*

Motor de Reglas monolítico

Para versiones inferiores a 3.6.7 el modelo tiene tres capas:

- Base de datos
- Capa de aplicación (API Server)
- Capa de administración (Backoffice + reportería)

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
> a 2.000.000	Consultar				

2024 VU Inc. Todos los derechos reservados.

Motor Reglas Modularizado (No incluye CEP)

El siguiente dimensionamiento se basa en la nueva arquitectura de Fraud Analysis en la que el motor de reglas CEP está modularizado.

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

2024 VU Inc. Todos los derechos reservados.

Soporte

Nivel de soporte

NUEVO

VU proveerá de soporte nivel 3.

El soporte provee un conjunto de tecnologías y derechos que tiene el cliente para ayudarlo a potenciar al máximo su inversión realizada en las licencias de VU.

Para contactarse con VU Support, enviar un correo a: customer.support@vusecurity.com

A partir de la recepción de su correo, se le asignará un caso de manera automática y recibirá todas las novedades relacionadas con su caso en el mismo hilo de correos.

En caso de querer agregar destinatarios, ponerlos en copia. Colocar en Asunto: [Nombre del cliente] [Criticidad] [Título del problema].

Los casos de soporte se tratan de **lunes a viernes de 9 a 18hs** (Argentina)

2024 VU Inc. Todos los derechos reservados.

Contactos

Otros productos de VU Security

Nuestras soluciones ofrecen una experiencia 360°, cada una aportando un aspecto fundamental a la estrategia de seguridad tanto de usuarios como de organizaciones.

Módulos de Onboarding Management:
• ID+Face
• Voice
• Touch

Authentication Management:
- Server
- SDK
- App

CIAM / IAM

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

2024 VU Inc. Todos los derechos reservados.

Acerca de VU

VU es una compañía global de ciberseguridad, especializada en protección de la identidad y prevención de fraude, que desarrolla soluciones modulares, fáciles de integrar y adaptables tanto al ámbito corporativo como gubernamental.

Para lograrlo, utiliza tecnologías innovadoras basadas en la combinación de controles tradicionales de ciberseguridad, biometría, geolocalización, inteligencia artificial, *machine learning*, reconocimiento de documentación y análisis del comportamiento del usuario.

Más de 350 millones de personas en todo el mundo y más de 130 clientes en 30 países de América Latina, Europa y Estados Unidos utilizan la tecnología de VU para digitalizar sus negocios y aumentar el nivel de operaciones reduciendo los riesgos de ataques y la pérdida de información.

Sus alianzas estratégicas con Microsoft, Telefónica, IBM, BGH, Intel, Cisco y Accenture, entre otras compañías, ayudan a VU a cumplir su misión: crear experiencias seguras y sin fricción que mejoren la calidad de vida de ciudadanos y organizaciones.

vusecurity.com

2024 VU Inc. Todos los derechos reservados.