Device & Browser Fingerprint

Reconocimiento de dispositivos confiables.

VU

Datasheet

Android V 1.4 / IOS V 1.4 / Cordova 1.1

Mayo 2025

¿Qué es?

Device & Browser Fingerprint constituye un módulo esencial dentro de **Fraud Prevention**, encargado de identificar la "huella digital" de los dispositivos utilizados por los usuarios al conectarse al sistema. Este proceso implica la recopilación de datos técnicos y propiedades de los dispositivos con el fin de prevenir el robo de identidad en línea y el fraude electrónico.

La capacidad para identificar y bloquear de manera rápida un dispositivo utilizado en actividades fraudulentas reduce significativamente la probabilidad de que se creen cuentas falsas o se realicen transacciones fraudulentas. Nuestra herramienta emplea datos como el modelo, la marca y el sistema operativo del dispositivo para alertar y evitar el robo de cuentas digitales antes de que se materialice cualquier actividad ilegal por parte de dispositivos no autorizados.

Device & Browser Fingerprint compara las "huellas digitales" de los dispositivos que intentan conectarse al sistema con los dispositivos asociados a usuarios legítimos del servicio. Luego, calcula la similitud y ejecuta las reglas de acceso y bloqueo previamente configuradas según corresponda en cada caso.

Beneficios

- Configura reglas sobre las transacciones para clasificarlas según su potencial de riesgo.
- Reconoce la confianza de usuarios, dispositivos y cuentas, incluso en navegación privada.
- Detecta y bloquea ataques fraudulentos antes de que afecten la reputación o las ganancias comerciales.
- Previene estafas en toda la experiencia del usuario, incluyendo suplantaciones de identidad y compras fraudulentas.
- Identifica cuentas mula mediante listas negras que incluyen cuentas sospechosas de ser utilizadas con fines fraudulentos.
- Puede implementarse como parte de una solución integral o como un módulo independiente que se integra con cualquier aplicación o sistema existente.

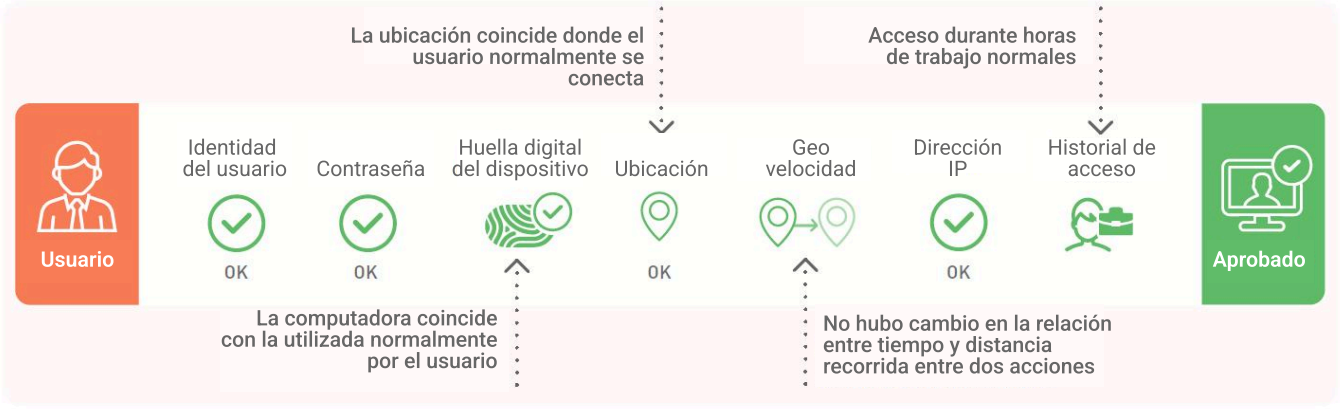
Algunos casos de uso más destacados

- Gestión de fuerza laboral, clientes y contratistas.
- Métodos de pago en línea, depósitos directos y tráfico de billeteras electrónicas.
- Verificación de enrolamiento e inicio de sesión de usuarios.
- Adquisición remota de entradas digitales, paquetes de viaje o servicios.

Proceso de validación del dispositivo

- **Device & Browser Fingerprint** obtiene la huella del dispositivo desde el que el usuario pretende conectarse al sistema.
- Compara esta información con los dispositivos conocidos para ese usuario y ejecuta las reglas previamente configuradas.
- Si el porcentaje de similitud obtenido coincide con los parámetros de autenticación predefinidos, se permite al usuario el acceso al sistema.
- Si el porcentaje de similitud no alcanza el umbral mínimo, se aplican las acciones definidas por las reglas.

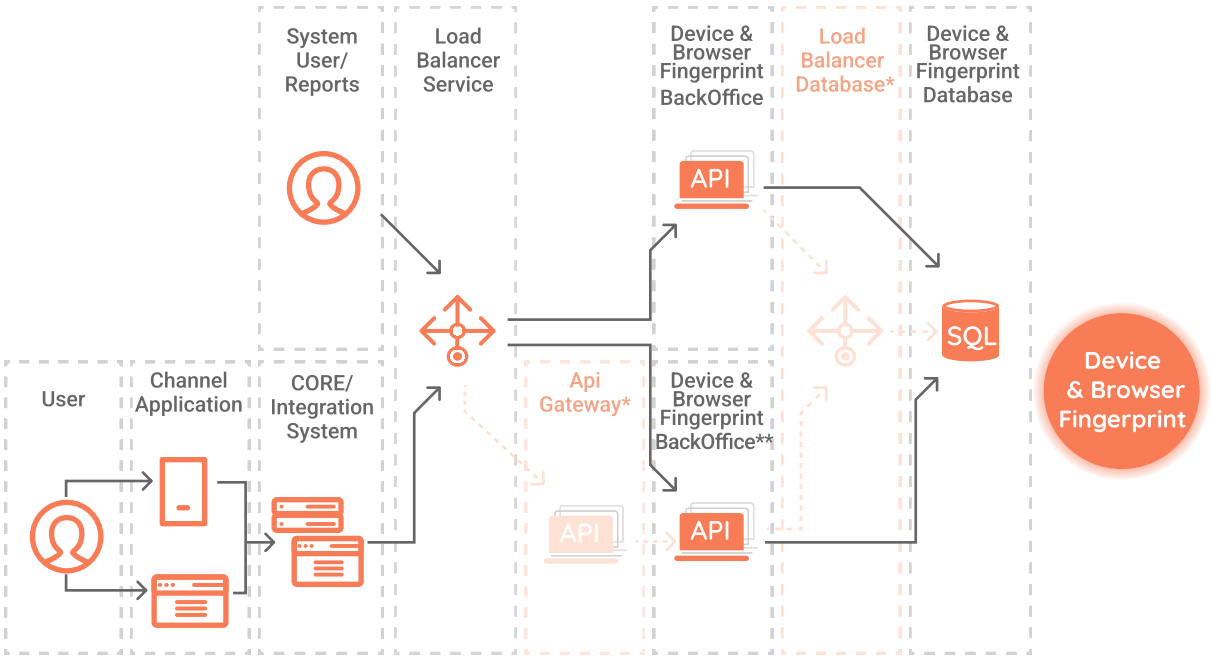
Autenticación positiva:



Autenticación negativa:

Diagramas lógicos de funcionamiento

Device & Browser Fingerprint 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.

Backoffice de Device & Browser Fingerprint

Device & Browser Fingerprint cuenta con todos los métodos necesarios para analizar todo tipo de transacciones o eventos:

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

Geolocalización del dispositivo
Define zonas geográficas seguras según el comportamiento habitual del usuario.

Panel de consultas
Gestiona casos y realiza seguimiento de posibles intentos de fraude en tableros personalizables.

Colección de Fingerprints
Agrupa incrementalmente todas las huellas digitales asociadas a un mismo usuario.

Detección en modo privado o incógnito
Identifica si un dispositivo intenta acceder al sistema desde una ventana de navegación privada.

Reportes y Analytics
Genera reportes predefinidos y personalizables.

SDK de Device & Browser Fingerprint

VU Security ofrece la capacidad de integrar la funcionalidad de **Device & Browser Fingerprint** en aplicaciones existentes de clientes o de terceros.
Para facilitar la implementación, proporcionamos un manual con ejemplos de todas las funciones, asegurando así una fácil adaptación al entorno real de uso, manteniendo siempre las condiciones necesarias para preservar la seguridad e integridad del producto.

- 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 Machine Learning.
- Descargar la información en archivos .CSV y/o PDF, XLSX.

Integración del SDK

Device & Browser Fingerprint puede integrarse en páginas web a través de un plugin de Javascript, pero además puede ser integrado en aplicaciones móviles a través de los siguientes SDK:

	Tecnología	Entrega
Android Java	**Java**	**SDK + Proyecto de ejemplo**
iOS	**Swift**	**SDK + Proyecto de ejemplo**
Web	**JavaScript**	**SDK + Proyecto de ejemplo**
Híbrido Ionic y Cordova	**JavaScript** Utilizan SDK Nativos (Swift y Java)	**SDK + Proyecto de ejemplo**

API de integración

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

Los métodos que componen la solución están diseñados para la administración de los usuarios finales. Estos permiten:

- Añadir, obtener y eliminar el fingerprint de un usuario.
- Etiquetar un fingerprint como válido o inválido.
- Comprobar si el dispositivo está dentro del umbral permitido.
- Establecer la necesidad de una autenticación de doble factor.
- Agrupar los fingerprints de un mismo usuario.

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

Información técnica

Requisitos y compatibilidad de software

Device & Browser Fingerprint 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 (*)(**)	Tomcat 9.0.54 o la versión inferior disponible (*)	Java JRE 11	iOS 11 o superior
PostgreSQL v13 o superior			Android 5 o superior

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

Dimensionamiento de hardware*

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				

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)

Fin de soporte extendido (EOS) y fin de vida (EOL)

	Soporte completo	Mantenimiento	Sólo soporte	Sin soporte
Pueden esperarse nuevas funcionalidades	✓	No	No	No
Corrección de errores	✓	✓	No	No
Soporte al cliente	✓	✓	✓	No

Versión de Fraud Analysis	Fecha de lanzamiento	Nuevas funcionalidades hasta	Correcciones hasta	Último día de soporte (LDOS)	Sin soporte desde
2.x	Enero 2015	N/A	N/A	N/A	Sin soporte
3.x	Enero 2018	Junio 2024	Junio 2025	Diciembre 2025	Enero 2026
5.x	Marzo 2022	Diciembre 2025	Diciembre 2026	Diciembre 2027	Enero 2028

Contacto

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

Otros productos de VU

- Authentication Management
  - Server
  - SDK
  - App
- Onboarding Management
  - ID
  - Face
  - Voice
  - Touch
- CIAM

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