VU

Device Fingerprint

Identifica las huellas de los dispositivos.

Datasheet

Android V 1.4 / IOS V 1.4 / Cordova 1.1

¿Qué es?

VU Device Fingerprint es un módulo de VU Fraud Analysis que funciona para identificar las huellas de los dispositivos mediante la recopilación de datos técnicos y propiedades de los dispositivos de los usuarios que seconectan a un sistema en línea. Identifica los dispositivos permitidos, genera reglas que detectan y previenen el robo de identidad en línea y el fraude electrónico. La huella digital del dispositivo se puede emplear para predecir la probabilidad de fraude, en función de su información de perfil.

Función Principal

La función principal de este módulo incluido en VU Fraud Analysis consiste en detectar el dispositivo desde el cual el usuario ingresó al sistema, y obtener de él cerca de 30 variables (campos parametrizables) que, en su conjunto, lo hacen único.

La información es obtenida mediante Javascript o a través de un SDK si se trata de una aplicación móvil. Dicho dispositivo y todas las características obtenidas del mismo se encuentran relacionadas a la cuenta del usuario. Por esta razón, a la hora de acceder al sistema con un nuevo dispositivo, el usuario tiene la posibilidad de agregarlo como un dispositivo conocido, tras haber validado su identidad con un doble factor de autenticación.

Una vez que se agrega el dispositivo y es vinculado con el usuario, cuando el usuario quiera acceder nuevamente al sistema, el módulo de Device Fingerprint compara las características del dispositivo conocido de ese usuario con una base de reglas predefinidas (detalladas más adelante en este documento), creadas desde la consola de administración de VU Fraud Analysis.
Este proceso detecta las variaciones en el login y su impacto sobre el porcentaje de semejanza para definir cuál de las siguientes acciones necesita realizar:

1. En el caso de que sea idéntico (100%), validar su identidad.
2. Verificar que el dispositivo esté dentro del umbral permitido (tomado como válido).
3. Determinar si requiere un doble factor de autenticación.
4. Ejecutar acciones previamente definidas en dicho módulo, si el umbral no supera el mínimo definido.

VU Device Fingerprint puede ser integrado a sus apps a través de los siguientes SDK:

- Android
- iOS
- Cordova

Plugin

VU Device Fingerprint puede ser integrado en páginas web utilizando Javascript.

Campos parametrizables destacados

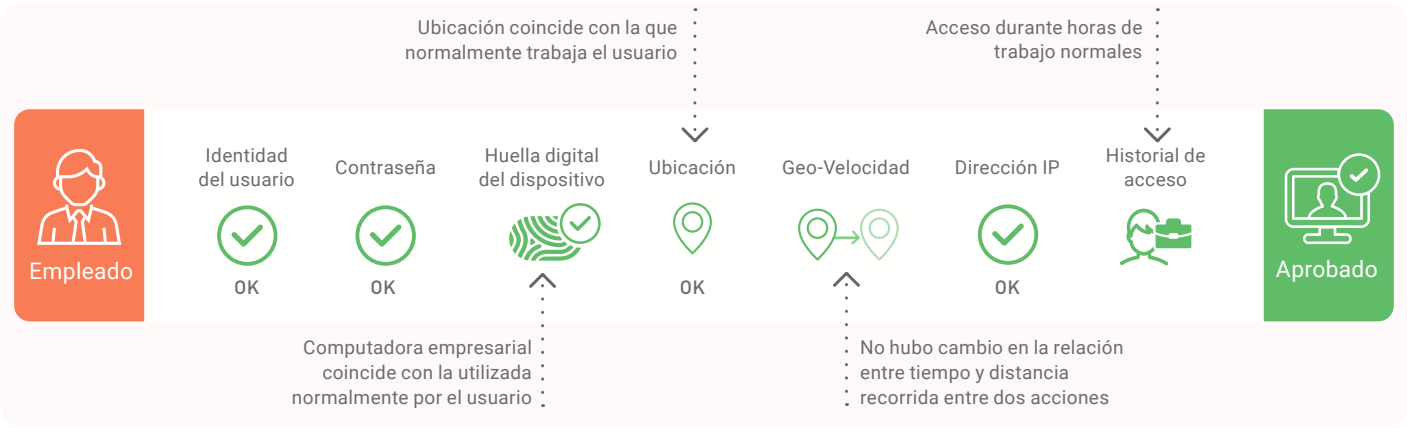
Estos son los parámetros que se pueden definir para crear las reglas y validar si la acción a ser realizada es fraudulenta o no:

Agente del Navegador	Lenguaje	Tipo de CPU
Color Depth	**Versiones**	**Sistema Operativo**
Sesiones	**Time Zone**	**Función “Donottrack”**
Plugins instalados	**Local Storage**	**WebGL Driver**
Resolución de Pantalla	**Fuentes**	**Cookies**

Ejemplos de casos de uso

En el diagrama a continuación presentado se muestran tres escenarios diferentes en los cuales Fingerprint obtiene la huella del dispositivo del usuario que desea conectarse al sistema, lo compara con los dispositivos conocidos del mismo y ejecuta las reglas que estén previamente configuradas para de esta forma obtener el porcentaje de semejanza y aprobar dicho acceso o tomar las acciones necesarias en el caso de que dicho porcentaje de semejanza no supere el mínimo predefinido anteriormente (explicado en la sección de reglas de este documento).

Escenario 1



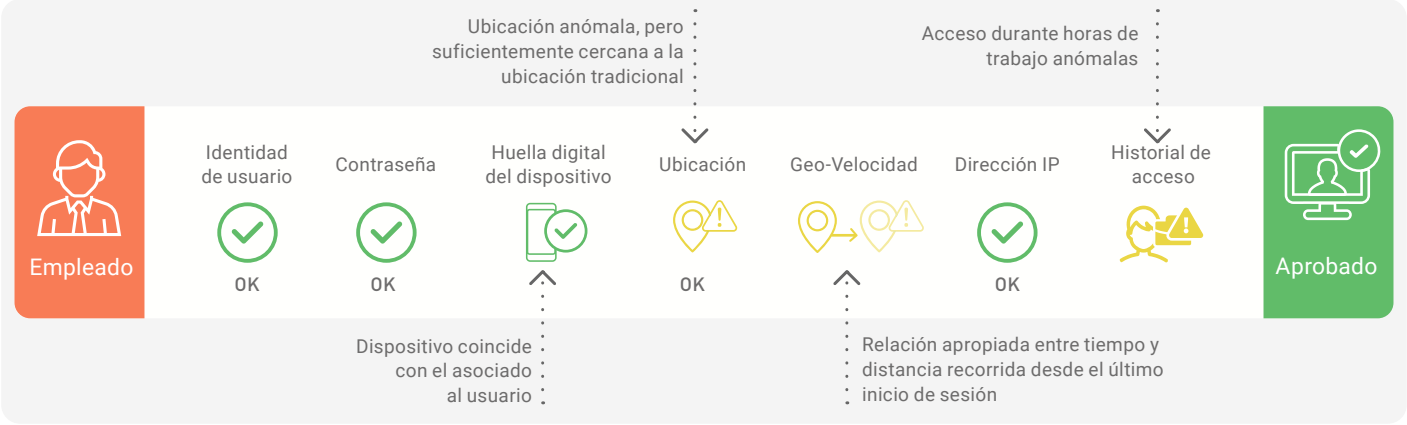
Situación:

El empleado legítimo intenta iniciar sesión para acceder a datos de la empresa desde su PC de trabajo en una oficina en el Sur de California a las 9 a.m. PST.

Autenticación positiva:

El empleado legítimo supera todas las validaciones mencionadas en la imagen y el porcentaje de semejanza de Fingerprint del dispositivo es de 100% (idéntico a un dispositivo conocido) por lo que el análisis de autenticación basada en el riesgo es positivo y la autenticación es aprobada para que el usuario pueda proseguir con la acción deseada.

Escenario 2



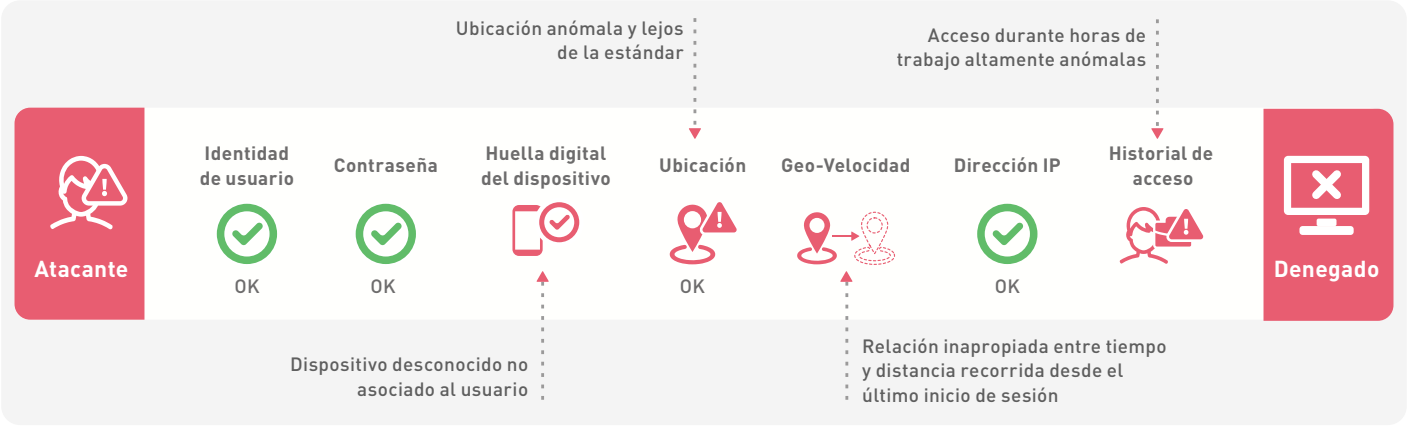
Situación:

El empleado legítimo intenta ingresar al e-mail corporativo en San Francisco a través de un smartphone a las 8.30 p.m. PST.

Autenticación positiva:

El empleado legítimo cambia de ubicación y accede a una hora anormal de trabajo, aunque valida su identidad y la huella del dispositivo es validada ya que pertenece a uno de sus dispositivos conocidos y agregados previamente por lo que según reglas predefinidas anteriormente el análisis de autenticación basada en el riesgo es positivo y la autenticación es aprobada para que el usuario pueda proseguir con la acción deseada.

Escenario 3



Situación:

El atacante intenta iniciar sesión para acceder a los datos corporativos del Reino Unido a través de una computadora personal a las 2 a.m. PST.

Autenticación positiva:

El atacante intenta iniciar sesión validando la identidad del usuario, pero la huella del dispositivo no coincide con ningún dispositivo conocido para ese usuario y se encuentra de una geolocalización lejos de la habituales por lo que el análisis de autenticación basada en el riesgo es negativo por lo que dicha autenticación falla y el usuario no puede realizar la transacción.

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