VU

Device Fingerprint

Identifique as impressões digitais dos dispositivos.

Datasheet

Android V 1.4 / IOS V 1.4 / Cordova 1.1

O que é o VU Device Fingerprint?

VU Device Fingerprint é um módulo do VU Fraud Analysis que trabalha para identificar impressões digitais de dispositivos coletando informações técnicas que permitem a identificação do dispositivo usado pelo usuário, cria regras que ajudam na prevenção do roubo de identidade online e fraudes eletrônicas. A impressão digital do dispositivo pode ser usada para prever a probabilidade de fraude com base nas informações do seu perfil.

Função principal

A principal função deste módulo que integra o VU Fraud Analysis é detectar o dispositivo a partir do qual o usuário entrou no sistema e obter dele cerca de 30 variáveis (campos parametrizáveis) que, como um todo, o tornam único.

As informações são obtidas através de Javascript ou de um SDK se for um app móvel. Este dispositivo e todas suas características estão relacionadas à conta do usuário. Desta forma, ao acessar o sistema com um novo dispositivo, o usuário tem a possibilidade de adicioná-lo como um dispositivo conhecido depois de ter validado sua identidade com um duplo fator de autenticação.
Uma vez que o dispositivo é adicionado e vinculado ao usuário, quando o usuário for acessar o sistema novamente, o módulo Fingerprint do dispositivo compara as características do dispositivo conhecido do usuário com uma base de regras predefinidas (detalhadas posteriormente neste documento) criadas a partir do console de gestão VU Fraud Analysis.

Este processo detecta as variações no login e seu impacto sobre a porcentagem de similaridade para definir quais das seguintes ações você precisa executar:

1. Caso seja idêntico (100%), valide sua identidade.
2. Verifique se o dispositivo está dentro do limite permitido (tomado como válido).
3. Determine se requer uma autenticação de dois fatores.
4. Execute ações previamente definidas nesse módulo se o limite não for superior ao mínimo definido.

O VU Device Fingerprint pode ser integrado aos seus aplicativos através dos seguintes SDKs:

- Android
- iOS
- Cordova

Plugin

O VU Device Fingerprint pode ser integrada em páginas da Web utilizando Javascript.

Campos parametrizáveis em destaque

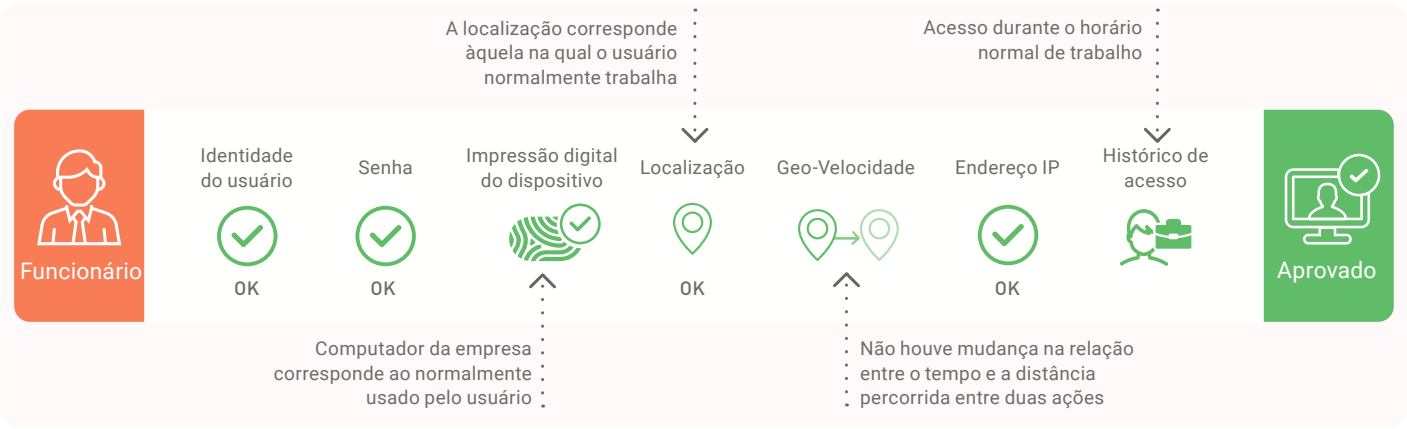
Estes são os parâmetros que podem ser definidos para criar as regras e validar se a ação a ser executada é fraudulenta ou não:

Agente do Navegador	Idioma	Tipo de CPU
Profundidade de cor	**Versões**	**Sistema operacional**
Sessões	**Fuso horário**	**Função “Donottrack”**
Plugins instalados	**Armazenamento local**	**Driver WebGL**
Resolução de tela	**Fontes**	**Cookies**

Exemplos de casos de uso

O diagrama abaixo mostra 3 cenários distintos em que o Fingerprint obtém a impressão digital do dispositivo do usuário que deseja se conectar ao sistema, compara-o com os dispositivos conhecidos do mesmo e executa as regras previamente configuradas para obter o percentual de similaridade, aprovar o referido acesso ou tomar as ações necessárias, caso essa porcentagem de similaridade não exceda o mínimo predefinido anteriormente (conforme explicado na seção de regras deste documento).

Cenário 1



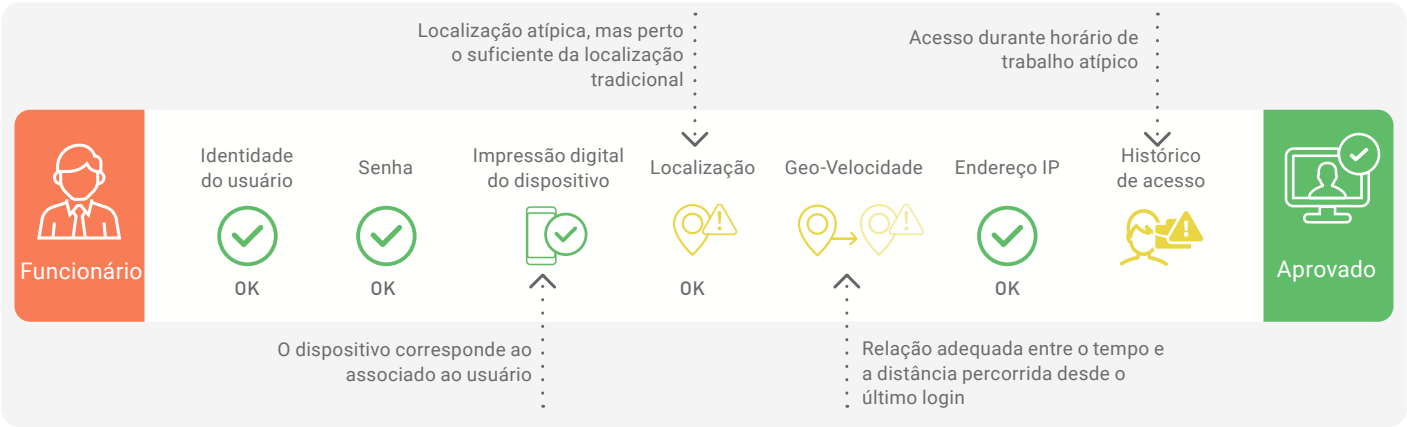
Situação:

O funcionário legítimo tenta fazer login para acessar dados da empresa de seu PC de trabalho em um escritório no sul da Califórnia às 9h, PST.

Autenticação positiva:

O funcionário legítimo passa por todas as validações mencionadas na imagem e a porcentagem de similaridade da impressão digital do dispositivo é de 100% (idêntica a um dispositivo conhecido). A análise de autenticação baseada em risco é positiva e a autenticação é aprovada para que o usuário possa prosseguir com a ação desejada.

Cenário 2



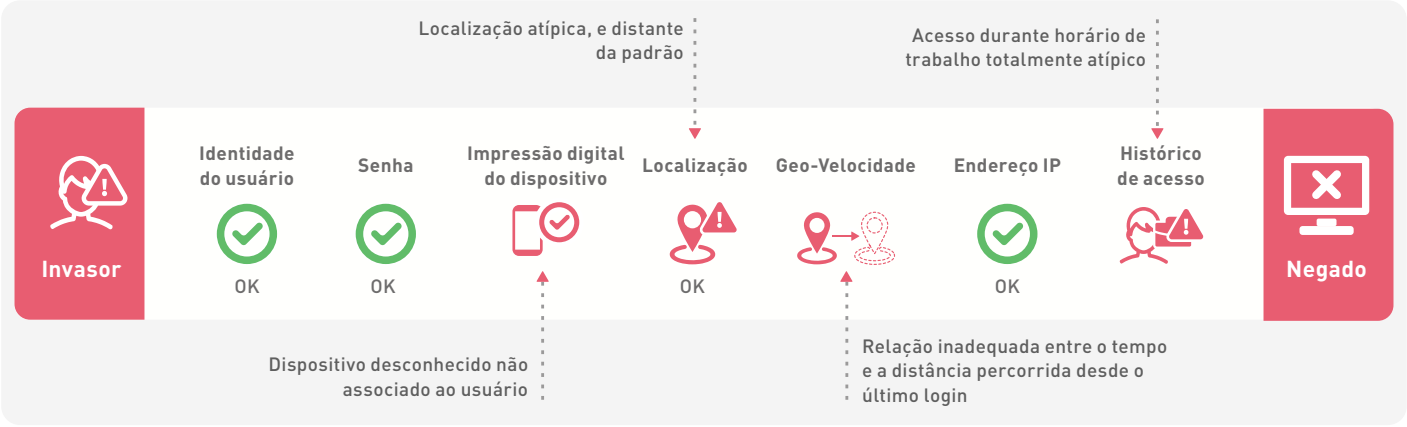
Situação:

O funcionário legítimo tenta fazer login no e-mail corporativo em São Francisco pelo celular às 20h30, PST.

Autenticação positiva:

O funcionário legítimo muda de local e acessa em horário anormal de trabalho, porém valida sua identidade e a impressão digital do dispositivo é também validada, uma vez que pertence a um de seus dispositivos conhecidos e adicionados anteriormente para que, de acordo com regras previamente predefinidas, a análise de autenticação baseada em risco seja positiva e a autenticação seja aprovada para que o usuário possa continuar com a ação desejada.

Cenário 3



Situação:

O invasor tenta realizar login para acessar dados corporativos no Reino Unido através de um computador pessoal às 2h, PST.

Autenticação positiva:

O invasor tenta fazer login validando a identidade do usuário, mas a impressão digital do dispositivo não corresponde a nenhum dispositivo conhecido desse usuário, em uma geolocalização distante da habitual, e por isso a análise de autenticação baseada em risco é negativa para que a autenticação falhe e o usuário não possa realizar a transação.

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