Device & Browser Fingerprint

Trusted device recognition.

Datasheet

Android V 1.4 / IOS V 1.4 / Cordova 1.1

April 2024

What is?

Device & Browser Fingerprint is an essential module within **Fraud Prevention**, responsible for identifying the "digital fingerprint" of the devices used by users when connecting to a system. This process involves the collection of technical data and device properties in order to prevent online identity theft and electronic fraud.

The ability to quickly identify and block a device used in fraudulent activities significantly reduces the likelihood of fake accounts being created or fraudulent transactions being carried out. Our tool uses data such as the device model, brand, and operating system to alert and prevent theft of digital accounts before any illegal activity can take place by unauthorized devices.

Device & Browser Fingerprint compares the "digital fingerprints" of devices that attempt to connect to the system with the devices associated with legitimate users of the service. It then calculates the similarity and executes the previously configured access and blocking rules accordingly in each case.

Benefits

- Establish rules for transactions to classify them based on their risk potential.
- Recognizes user, device, and account trust, even in private browsing.
- Detects and blocks fraudulent attacks before they impact reputation or business profits.
- Prevents scams throughout the user experience, including phishing and fraudulent purchases.
- Identifies mule accounts using blacklists that include accounts suspected of being used for fraudulent purposes.
- Can be implemented as part of an integrated solution or as a standalone module that integrates with any existing application or system.

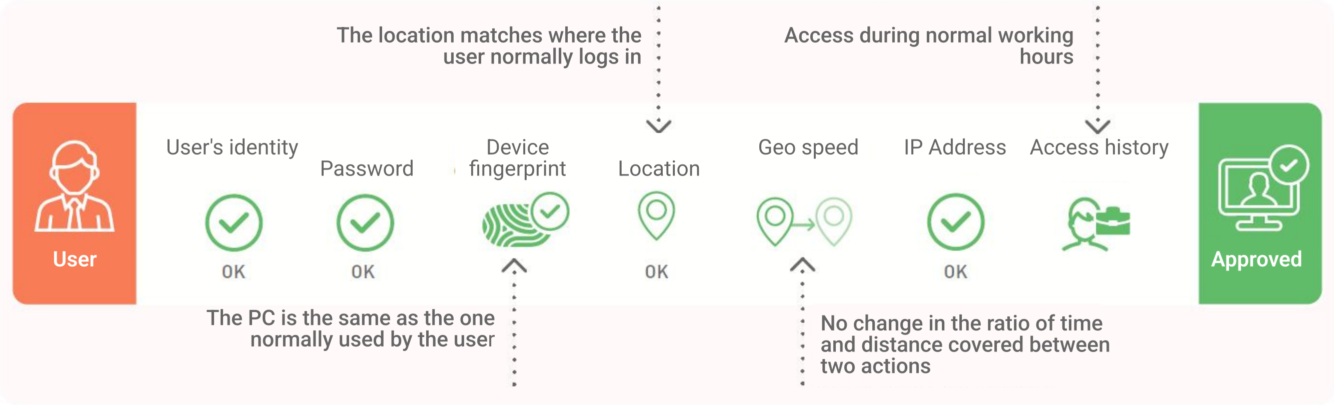
Outstanding use cases

- Workforce, customer, and contractor management.
- Online payment methods, direct deposits, and e-wallet traffic.
- User enrollment and login verification.
- Remote acquisition of digital tickets, travel packages, or services.

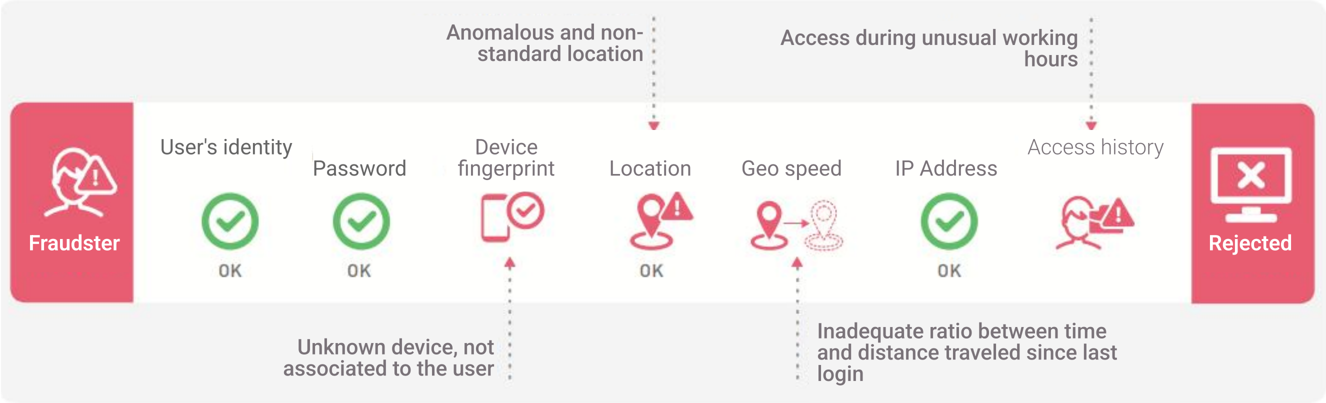
Device validation process

- **Device & Browser Fingerprint** retrieves the device's fingerprint from which the user intends to connect to the system.
- It compares this information with the known devices for that user and executes the previously configured rules.
- If the obtained similarity percentage matches the predefined authentication parameters, the user is allowed access to the system.
- If the similarity percentage does not reach the minimum threshold, the actions defined by the rules are applied.

Positive authentication:

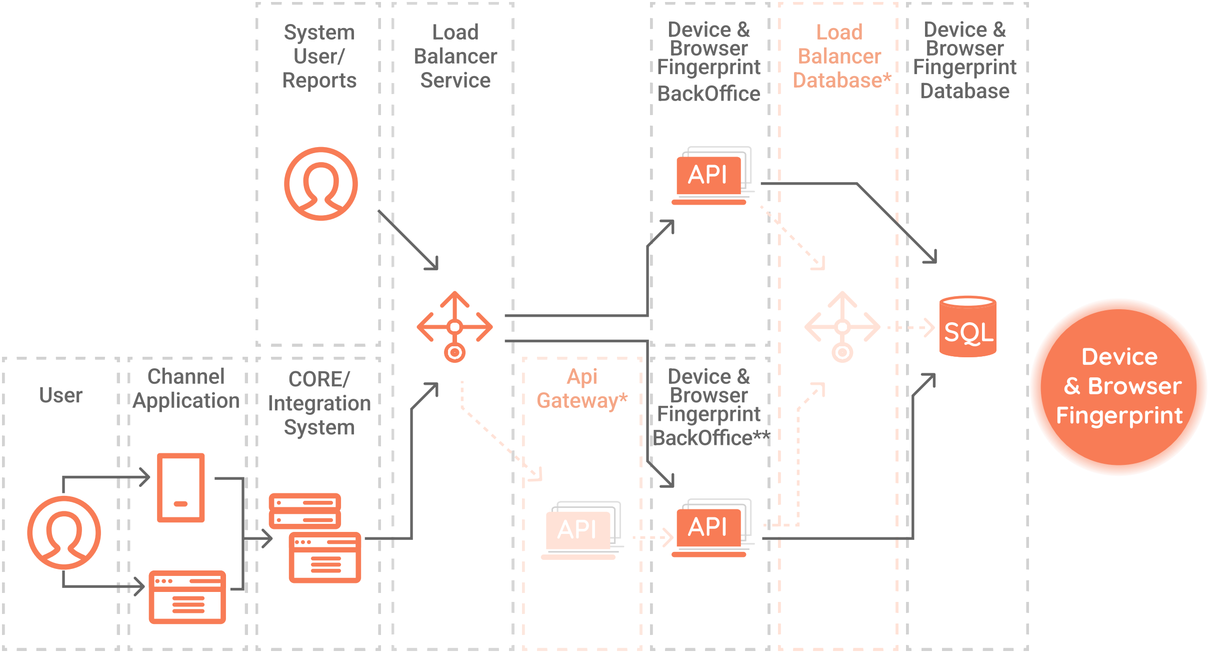

The location matches where the user normally logs in
Access during normal working hours
User
User's identity
OK
Password
OK
Device fingerprint
Location
OK
Geo speed
IP Address
OK
Access history
Approved
The PC is the same as the one normally used by the user
No change in the ratio of time and distance covered between two actions

Negative authentication:


Anomalous and non-standard location
Access during unusual working hours
Fraudster
User's identity
OK
Password
OK
Device fingerprint
Location
OK
Geo speed
IP Address
OK
Access history
Rejected
Unknown device, not associated to the user
Inadequate ratio between time and distance traveled since last login

Operating logic diagram

Device & Browser Fingerprint can be obtained as a cloud service or through software licensing (on-premises) or hybrid deployment.


System User/ Reports
Load Balancer Service
Device & Browser Fingerprint BackOffice
Load Balancer Database*
Device & Browser Fingerprint Database
API
SQL
Device & Browser Fingerprint
User
Channel Application
CORE/ Integration System
Api Gateway*
Device & Browser Fingerprint BackOffice**
API
API

** Optional*

*** CEP requires a license to work with more than one node*

Focus on user experience

At **VU Security**, we understand the importance of user experience in cybersecurity solutions. Tools should be built with users' everyday lives in mind, helping them understand, use, and benefit from the product.
In response to this need, we have designed a user-centric solution that makes it easy for fraud analysts to identify suspicious transactions and visualize risk alerts.

Device & Browser Fingerprint Backoffice

Device & Browser Fingerprint offers all the necessary methods to analyze all types of transactions and events:

Rules Engine
Executes real-time actions based on predefined and customizable rules.

Device Geolocation
Defines secure geographic zones based on the user's typical behavior.

Query Dashboard
Manages cases and tracks potential fraud attempts on customizable dashboards.

Fingerprint Collection
Groups all fingerprints associated to the same user in an incremental way.

Private or Incognito Mode Detection
Identifies if a device attempts to access the system from a private browsing window.

Reports and Analytics
Generates predefined and customizable reports.

Device & Browser Fingerprint SDK

VU Security offers the capability to integrate the functionality of **Device & Browser Fingerprint** into existing client or third-party applications.
In order to facilitate the implementation, we provide a guide with examples of all functions, ensuring an easy adaptation to the real use environment, always maintaining the necessary conditions to preserve the safety and integrity of the product.

- Alert and block suspicious transactions.
- Configure rules to define fraudulent transactions and events.
- Generate dynamic reports by channels, users, and rules.
- Recognize user's typical behavior with Predictive Models.
- Download information in .CSV and/or PDF, XLSX file formats.

SDK integration

Device & Browser Fingerprint can be integrated into web pages through a Javascript plugin, but it can also be integrated into mobile applications through the following SDKs:

	Technology	Deliverable
Android Java	**Java**	**SDK + Sample project**
iOS	**Swift**	**SDK + Sample project**
Web	**JavaScript**	**SDK + Sample project**
Hybrid Ionic and Cordova	**JavaScript** It uses natives SDKs (Swift and Java)	**SDK + Sample project**

Integration API

The solution's infrastructure is designed to integrate with any other platform, regardless of the language used, through REST API services. Communication between the server and the application is done through an SSL/TLS connection.

The methods that make up the solution are designed for the administration of the end users. They allow to:

- Add, obtain, and delete a user's fingerprint.
- Flag a fingerprint as either valid or invalid.
- Check if the device is within the allowed threshold.
- Establish the need for a two-factor authentication.
- Group a same user's fingerprints.

It is carried out using REST methods, always using a secure SSL channel (port 443).

Technical information

Hardware and software requirements

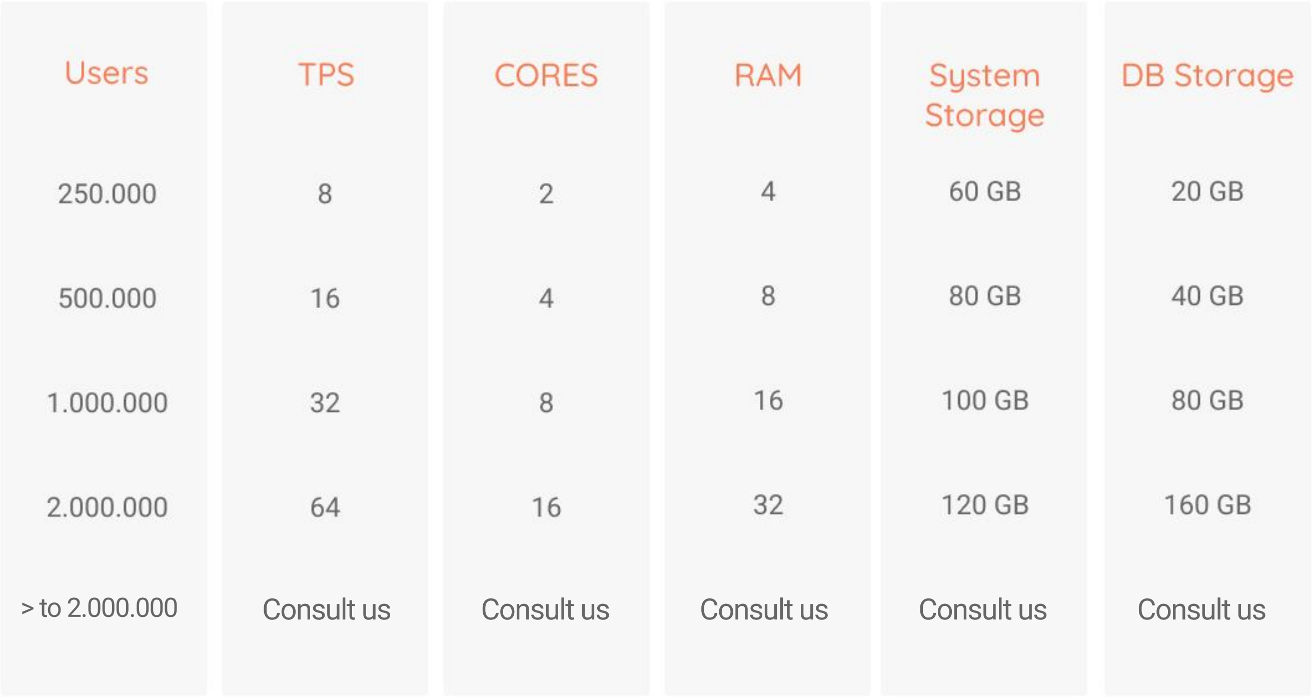
Device & Browser Fingerprint has a framework with extensive integration capabilities with different systems, such as Microsoft and Cisco, among others.
It allows the creation of predictive models to optimize the process, analyze different types of events and reduce transactional fraud.

Database	App Server	Java	Devices compatibility (SDK)
MS SQL 2017 or higher (*)(**) Oracle 18.0 or higher PostgreSQL v13 or higher	Tomcat 9.0.54 or the lower version available (*)	Java JRE 11	iOS 11 or higher Android 5 or higher

(*) Recommended

(**) Supplied in the installation packages.

Hardware sizing*



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
> to 2.000.000	Consult us	Consult us	Consult us	Consult us	Consult us

Support

Support level

VU Security will provide **level 3 support**.

Support includes a set of technologies and rights to help the customer maximize the investment made in VU Security licenses.

To contact VU Security support team, please send an email to: customer.support@vusecurity.com

As soon as your email is received, you will be automatically assigned a case and you will receive all the news related to your case in the same email thread.

If you want to add recipients, put them on a copy. Put Subject: [Name of the client] [Criticality] [Title of the problem].

Support cases are dealt with from **Monday to Friday from 9 a.m. to 6 p.m.** (Argentina).

Other VU Security products

Our solutions offer a 360° experience, each contributing an essential aspect to the security strategy of both users and organizations.

Onboarding Management:

- ID+Face
- Voice
- Touch

Authentication Management:

- Server
- SDK
- App

CIAM / IAM

Contact

If you need more information or want to schedule a demo of this solution, please write to us at: sales@vusecurity.com

About VU Security

VU is a global cybersecurity company specializing in identity protection and fraud prevention. We develop modular, easy-to-integrate solutions that are adaptable for both corporate and government sectors.

To achieve this, we utilize innovative technologies that combine traditional cybersecurity controls with biometrics, geolocation, artificial intelligence, predictive models, document recognition, and user behavior analysis.

More than 350 million people worldwide and over 130 clients in 30 countries across Latin America, Europe, and the United States rely on VU Security's technology to digitize their businesses and enhance operational efficiency while reducing the risks of attacks and information loss.

Our strategic alliances with Microsoft, Telefónica, IBM, BGH, Intel, Cisco, Accenture, and other companies contribute to VU Security's mission: to create secure and frictionless experiences that improve the quality of life for individuals and organizations.

vusecurity.com