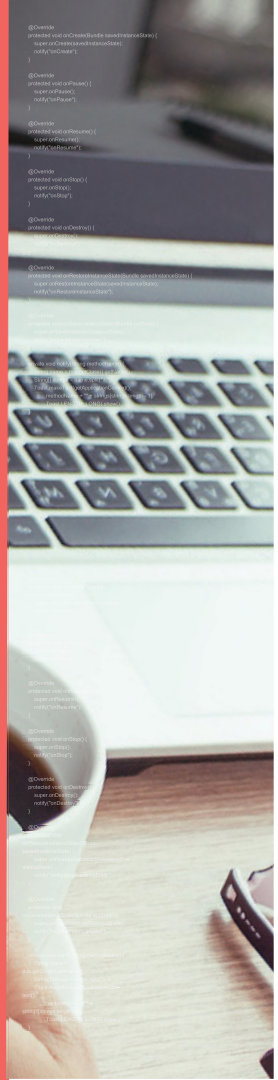
VU Fraud Analysis®



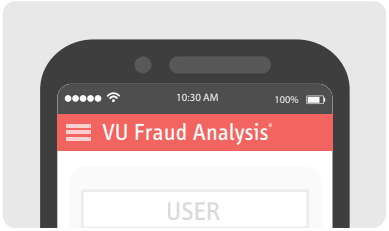
What is it?

It is a multi-channel fraud prevention solution that uses Machine Learning to create smart profiles and prevent fraud. It creates alerts of a possible fraud when a transaction goes out of the usual parameters.

Benefits

- It sets rules for transactions, so they are classified according to their potential risk.
- It receives information from different channels and does not need technical knowledge for its administration.
- It collects the registered virtual fingerprints to compare them against the company's database.
- It evaluates safe zones for each user based on their route, transaction times and device geolocation for each transaction.

Differentials



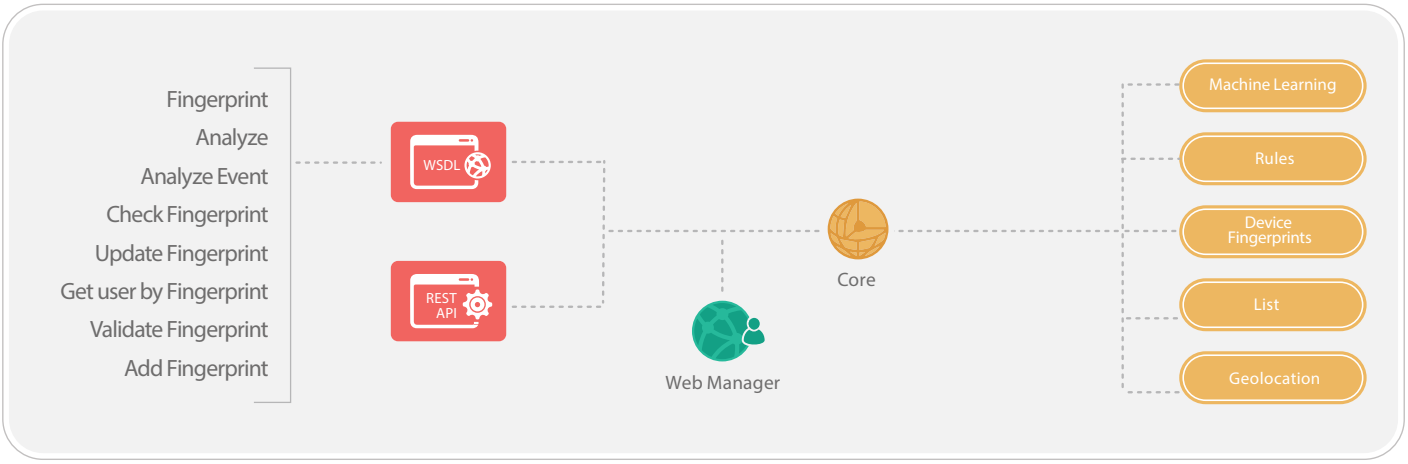
- Its sucess rate is over 95 percent.
- Integrated with VU Mobile Tokens, it evaluates information both online and offline, and uses VU Comm to send notifications to customers or internal staff
- It enables the end user to manage his own rules of usual behavior and fraud exceptions, for example.

VU Fraud Analysis®

About VU Fraud Analysis®

It is a fraud prevention multichannel solution that uses machine learning to create smart profiles and prevent fraud. It sends alerts whenever it detects a transaction made beyond the regular values.

It sets the standards on which the different transactions are classified, according to their risk potential. It gathers registered digital prints and compares them with its own base. It receives information from a variety of channels, and it does not require technical knowledge for its management. On each transaction, it evaluates safe areas for each user, considering their routes, transaction times and the device's geolocation.



Software requirements and compatibility

Operating System

Debian 7 or higher
Ubuntu 14.04 or higher
Red Hat RHEL 6 or higher
Suse 10 or higher
Solaris 10 x86
Solaris 10 Sparc
Windows 2008 R2 or higher

Databases

MySQL 5.6 or higher
PostgreSQL 9 or higher
Oracle 10 or higher
MS SQL 2008 or higher
MS SQL 5.6 or higher
MariaDB 5.5 or higher
DB2

Virtualization

VMWare
Citrix
Microsoft Hyper-V
RHEV
Virtual Box
Docker

High Availability

HA Proxy
KEEPALIVE
REPMGR
DRBD

Browsers

Firefox
Internet Explorer 10 or higher
Google Chrome
Apple Safari

Technologies

Java 1.7 or higher

Security

RSA / SHA1 / 3DES / AES 256
Security Certificates
EAP-PEAP-MSCHAP v2
TimeStamp
HOTP/OCRA/TOTP/HMAC

Web Server

Apache 2
Nginx
IIS
Weblogic
Jboss
Tomcat
WebSphere

Integrations	Access Management	Register & Report Management	Mobile OS
WS-I Basic Profile 2.0 SOAP 1.1 or higher WSDL 1.1 / WS-Security WSI XML Schema 1.0 TSL 2.0	Radius Cisco ACS 4.2 or higher FreeRadius Active Directory Samba Cisco ISE	Crystal Reports Syslog Nagios	iOS, Android, Windows Phone, HTML5, USSD SMS, Push Notification

Technical Information

Device Fingerprint SDK

VU provides the possibility of adding Device Fingerprint to existent applications. Device Fingerprint is the digital fingerprint of the device from which the transactions are being made. This piece of information is usually of an utter importance when it comes to detect fraudulent maneuvers.

The Device Fingerprint SDK offers every method clients need to use it for:

- **Registration**
- **Authentication**

These allows VU to add it to its clients' applications, besides maintaining the necessary conditions to preserve the product's security and integrity.

To improve the SDK deployment, a guide containing examples of the use of every function is delivered, so as to make the execution on a real scenario easier.

The SDK is developed on Java for Android, on Objective-C for iOS (compatible with Swift) and on JavaScript, which makes it possible to run on Web and Mobile hybrid developments, such as Cordova/ Phonegap.

For Android, it compiles a project developed on Android Studio containing the SDK in the libs directory as an Android Archive (.aar), already attached to the project. This way, the file can be copied and incorporated to the client's project. At the same time, a Java Archive (.jar) can be delivered in case the client uses another Android development environment.

For iOS, it compiles an Objective-C project created on Xcode, with the SDK library in .a format, ready to work with all the available iOS architectures.

For Web or hybrid development, it compiles a Web HTML site that uses the SDK developed on JavaScript, along the required JavaScript premises.

Integration API

The integration infrastructure is designed to merge with any other platform, no matter its language, used through Web services (WSDL) published on VU App & Cloud Server®.

The application is composed of different methods, identified with functions destined to the administrative management and the use of final users. The communication between the presentation layers and the VU App & Cloud Server® is made with an SSL connection.

The available methods can:

- Analyze transactions
- Analyze events
- Link a Fingerprint to a user
- Validate a user's Fingerprint
- Find a user through a Fingerprint

Hardware Sizing*

Primary Instance		Secondary Instance			
Processor	**Memory**	**Processor**	**Memory**	**Transactions per second**	**Storage required**
4 processing threads	4 GB RAM	4 processing threads	4 GB RAM	20	60 GB - HD
8 processing threads	8 GB RAM	8 processing threads	8 GB RAM	40	120 GB - HD
16 processing threads	16 GB RAM	16 processing threads	16 GB RAM	80	240 GB - HD
32 processing threads	32 GB RAM	32 processing threads	32 GB RAM	160	480 GB - HD
64 processing threads	64 GB RAM	64 processing threads	64 GB RAM	320	1 TB - HD

* The present sizing estimation assumes a high availability setup.