RAID.Cloud

Fraud Management in the cloud

for Communications Service Providers

WeDo technologies

Know the unknown

5 Good Reasons for choosing **RAID.Cloud**

Fast implementation time, providing quick access to Apps

Scalability to support changing business needs and future growth

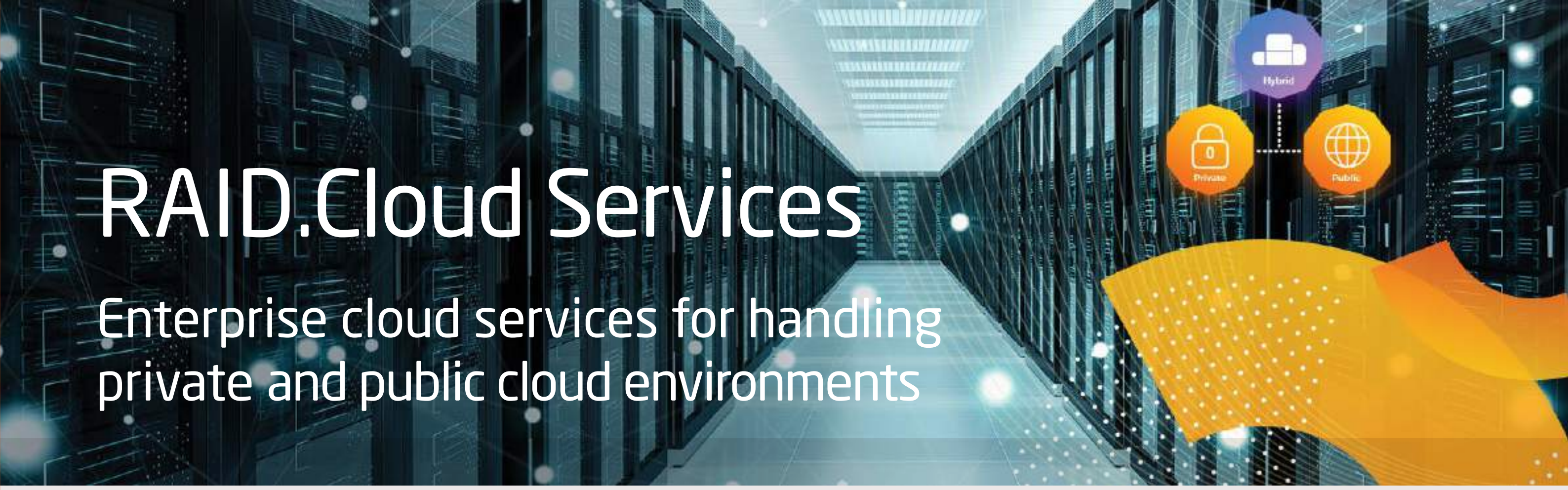
Subscription model provides "pay-per-use" flexibility

Reduced IT efforts, because both hardware and software operations and maintenance are WeDo Technologies' responsibility

60 day free trial

Scan this QR code
to access your 60 day free trial

RAID.Cloud



RAID.Cloud Services

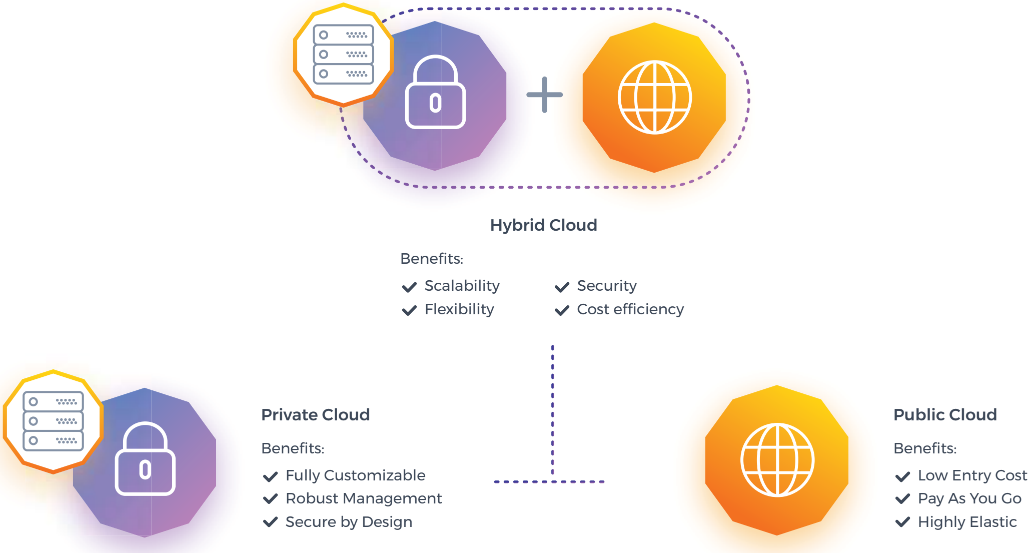
Enterprise cloud services for handling private and public cloud environments

For some CSPs with on-premise technology infrastructure, operating in a hybrid architecture is a necessary part of their cloud adoption roadmap. If your company still doesn't have a full public cloud policy due to security and compliance issues, WeDo Technologies provides an alternative private and hybrid cloud model to deploy prebuilt RAID.Cloud risk management apps.

The co-located hybrid cloud approach means that all data is stored on the private cloud, and it has the advantage of being behind firewalls at all times, even during transmission. Performance loss due to latency over WAN links is avoided too, as is the elapsed time involved in making data replicas in the public cloud and then keeping them synchronized.

RAID.Cloud private cloud appliances are a totally integrated infrastructure system engineered to enable rapid deployment of converged computing when it comes to our fraud management applications. With RAID.Cloud option models, you can deploy the Fraud Management Apps on your private on-premise cloud in minutes, configure cloud-based services or add more fraud management applications, and choose if you want to scale to public or hybrid cloud environments in the near future.

RAID.Cloud offers a family of hybrid and cloud appliances to support your IT needs.



Hybrid Cloud

Benefits:

- ✓ Scalability
- ✓ Flexibility
- ✓ Security
- ✓ Cost efficiency

Private Cloud

Benefits:

- ✓ Fully Customizable
- ✓ Robust Management
- ✓ Secure by Design

Public Cloud

Benefits:

- ✓ Low Entry Cost
- ✓ Pay As You Go
- ✓ Highly Elastic

Benefits

Open Source

Powered by OpenStack, a leading open source Infrastructure as a Service (IaaS) provider

Adaptable

Adapt your cloud strategy to suit your needs – not something you can do with other vendors in the market!

Scalable

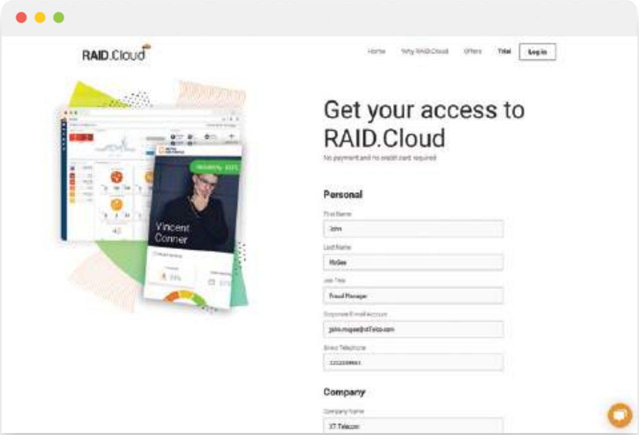
Scale-up or down as demand dictates, to better manage resources

Predictable

RAID.Cloud delivers predictable and dependable performance through design and optimization for all of your workload needs.

Fraud Management-as-a-Service:
beyond the Next Generation FMS

Main Features



Get your access to RAID.Cloud

No payment and no credit card required

Personal

First Name: John

Last Name: McGee

Job Title: Fraud Manager

Corporate E-mail Account: john.mcgee@xTelco.com

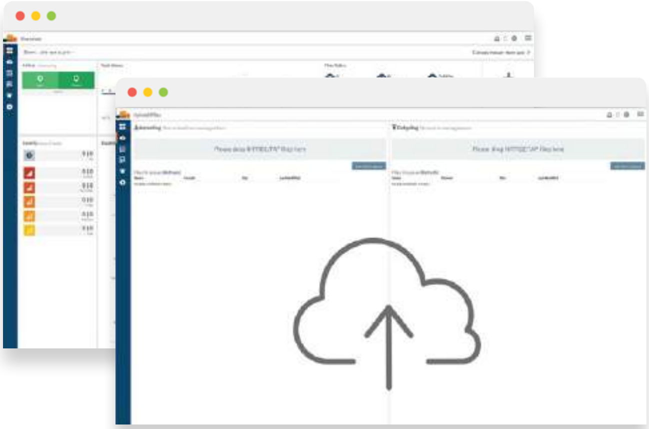
Direct Telephone: [illegible]

Company

Company Name: XT Telecom

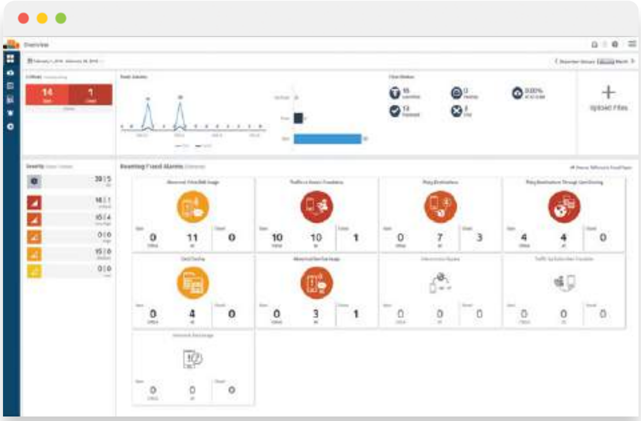
Free. Unlimited. Online.

It only takes 5 minutes to enroll on RAID.Cloud's 60 day free trial. Register on the website, select the app you want to use and submit the information. Our customer success team will immediately get in touch with you to help you setup so you can start processing data in a matter of minutes. Invite your team mates and get the full experience of the system working in near-real-time without any restrictions.ORIt takes only 5 minutes to start using RAID. Cloud's 60 day free trial. Just register through our website and select the apps you want to use. Our customer success team will respond immediately and then you can start processing your data in a matter of minutes. Invite your team mates and experience the system in full without any restrcitions, in near-real-time.



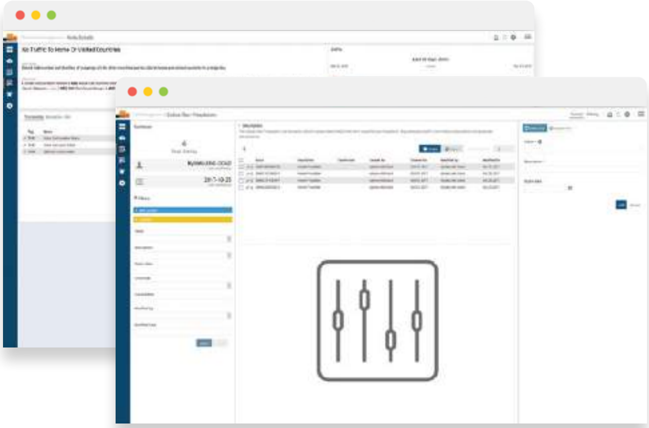
Data uploads made easy

RAID.Cloud gives you the convenience of processing data directly from the user interface or from a secure FTP. Once you've requested access to an app through the RAID.Cloud website, you will receive your unique personal authentication credentials for the dedicated secure FTP (sFTP). Each app comes with clearly defined file formats and our data transformation services is included in the free trial, so that you don't experience any delays in testing the solution.



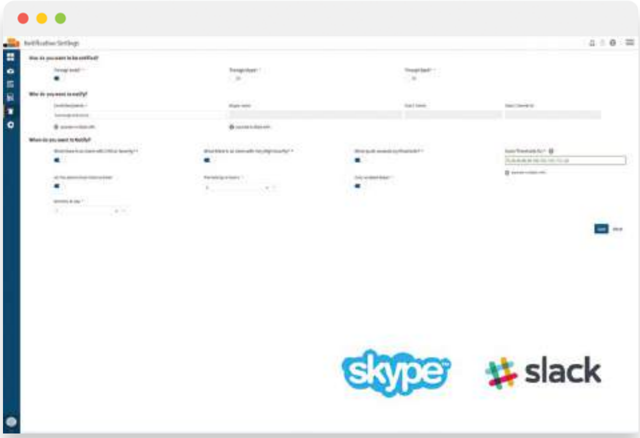
Quick access to your most important business metrics

All of the fraud apps start producing results immediately on top of your processed data. The easy-to-use dashboard also displays two ways of looking at the alarms generated, allowing you to see results either as fraud types or fraud patterns. RAID.Cloud allows you to drill down on the alarms, enabling you to identify patterns and behaviors, as well as to investigate cases by comparing against previous periods while trying to understand what triggered the alarms.



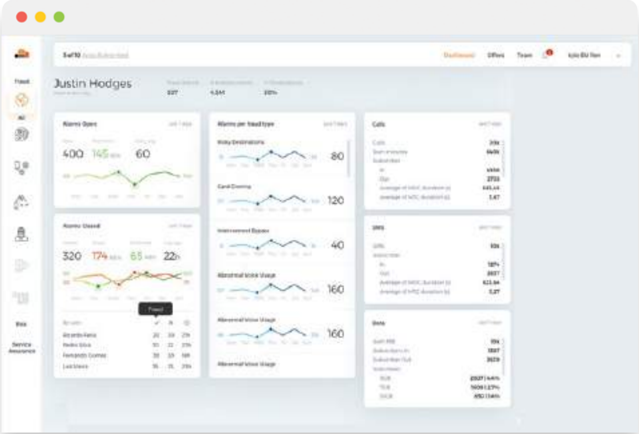
Fine-tune for extreme accuracy

RAID.Cloud provides prebuilt rules with default thresholds for fraud detection. Unlike other black box systems in the market, these values are fully customizable to help you to reduce potential false positives. Exceptions Management and Hotlists are also available, and constantly updated, to enhance accuracy by allowing you to add your own fraudsters, risky destinations or IMEIs in the application.



Easy to set-up notifications will keep all of your team informed

All apps utilize an intuitive dashboard which allows you to setup different alarms according to the severity, pattern or type of fraud. Taking advantage of the latest communication techniques designed to help you to reduce workloads and increase efficiency, RAID.Cloud provides notifications through email, Slack and Skype. You have full control over who, when and how you want to be notified.

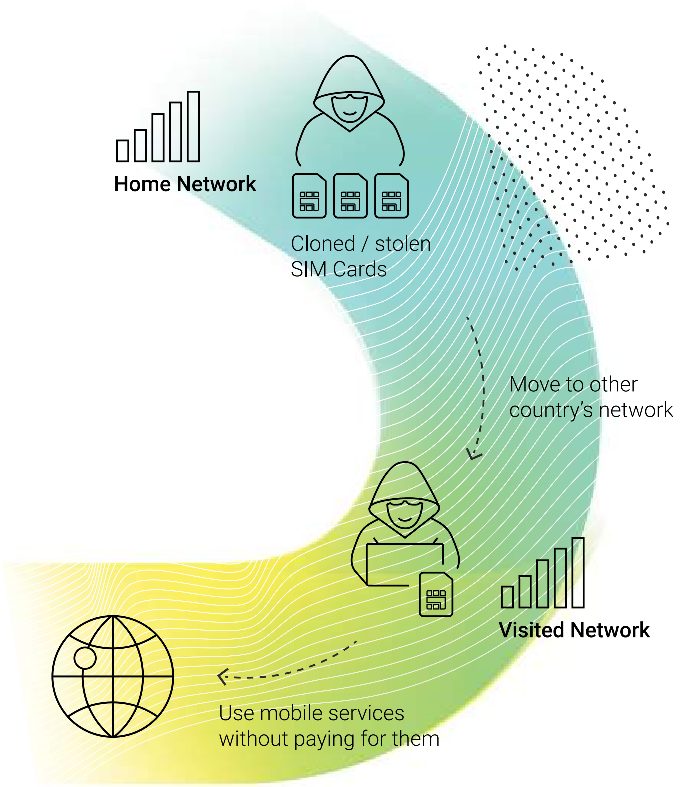


An integrated vision of how you are addressing fraud risks

RAID.Cloud provides a consolidated dashboard for evaluating results across multiple subscriptions. This lets you better understand fraud attacks and follow their outcomes and resolutions from a single point of access. By tracking all of your statistical data, you are also able to analyze fraud over multiple time frames and determine your level of protection. RAID.Cloud gives you the power to address all your needs in just one place.

Roaming Fraud

Roaming fraud is the most common type of fraud committed by those roaming on the Visited Public Mobile Network (VPMN). It occurs when a subscriber moves from their home network onto another operator's network, and then uses their services with no intention of paying, making the home network responsible for the charges.


Home Network
Cloned / stolen SIM Cards
Move to other country's network
Visited Network
Use mobile services without paying for them

This type of fraud can be perpetrated in several ways, the most common being:

Subscription Fraud

Fraudulent access to SIM cards from within one or more service providers or networks.

Time Delays

Fraudsters take advantage of time delays that occur during the interchange of roaming data between network operators.

Traffic Pumping

Artificially generating and 'pumping' large amounts of traffic through high-tariff international numbers, typically located in small or remote countries or via international satellite operators. (also known as International Revenue Share Fraud (IRSF)).

Keeping a Low Profile

Spreading fraudulent use across several operators within the same country, with the purpose of staying below the thresholds agreed between roaming partners.

Secure your roaming revenues by eliminating fraud.

Get your 60-Day Free Trial

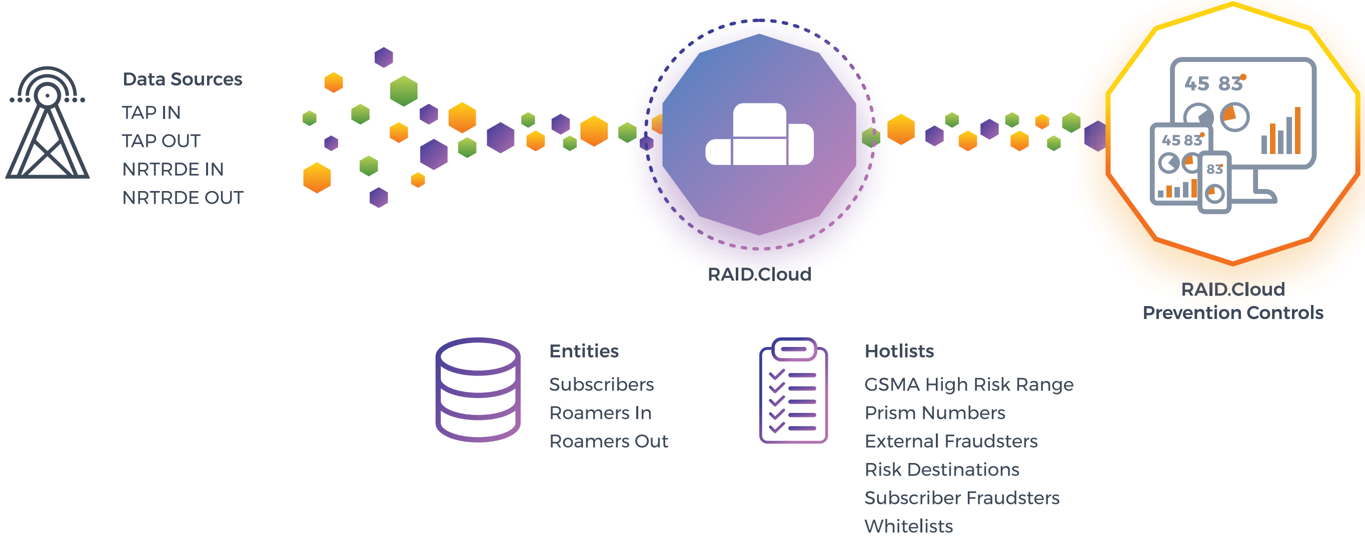
*60 Days free trial only available for Telecom Operators.

Some of the Apps' availability may depend on the region.

These behaviors are particularly damaging to the home operator, since it results in costs that can create significant revenue loss.

The RAID.Cloud Roaming Fraud App is a pre-configured Fraud Management Application that allows you to audit and control Inbound and Outbound network traffic. By analyzing TAP and NRTDE files, we identify fraud trends and uncover new fraud patterns. Its near real-time performance ensures that activities which are breaking defined rules, thresholds and profiles are identified almost immediately, enabling service providers to act fast to determine if the case is fraudulent.

How does our app work?



International Revenue Share Fraud

International Revenue Share Fraud is generally initiated by fraudulent traffic activity generated on a network that causes payments to another network or PRS provider, however in these fraud scenarios, the subsequent revenues will not be collect for those events.

The most common scenarios which undermine an operator's ability to monitor this are:

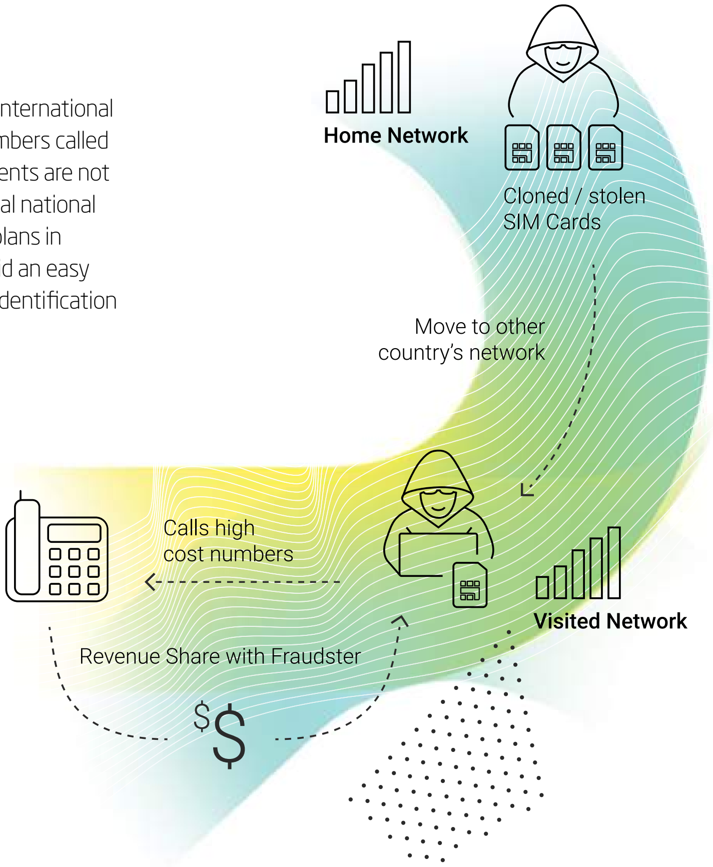
The generation of calls to a certain international or premium number or range of numbers, artificially inflates the traffic with no intention to pay for the calls.

The fraudster receives a share of the revenue generated by the termination charges obtained for inbound traffic of the international or premium number ranges called.

Usually the international and PRS numbers called in IRSF incidents are not part of official national numbering plans in order to avoid an easy B-numbers identification like PRS.

IRSF can also be perpetrated by targeting destinations on the national numbering plan with high termination rates, although these calls are often stopped quickly.

IRSF is commonly carried out in conjunction with subscription fraud, PBX hacking or SIM cloning in order for the fraudster to obtain access to the network services required to generate calls.


Home Network
Cloned / stolen SIM Cards
Move to other country's network
Calls high cost numbers
Visited Network
Revenue Share with Fraudster
$

Develop a protective barrier to unwanted premium-rate termination calls

Get your
60-Day
Free Trial

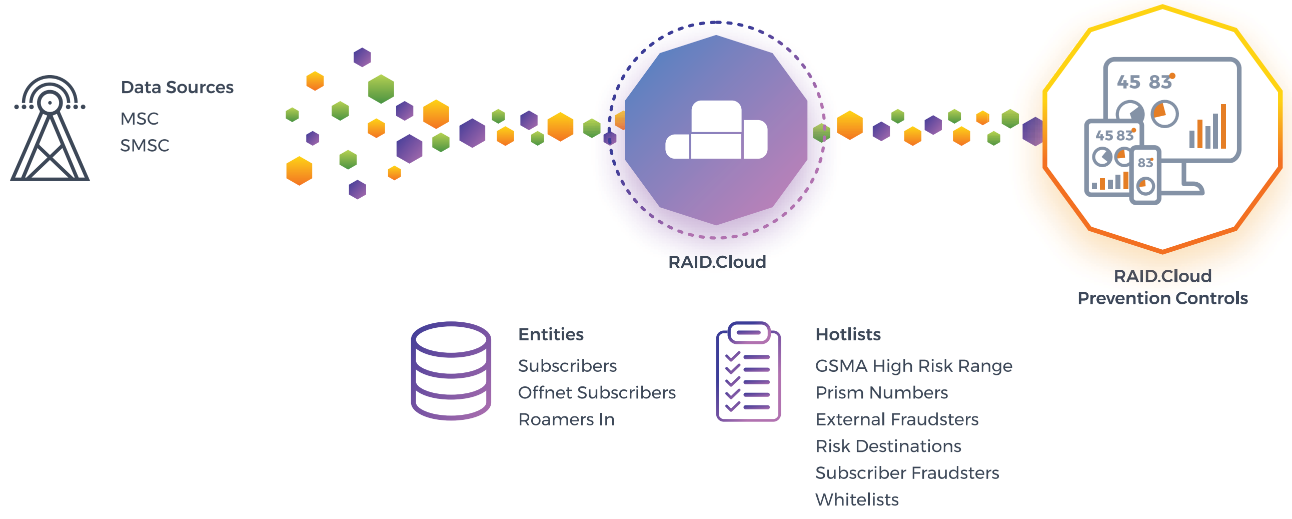
*60 Days free trial only available for Telecom Operators.

Some of the Apps' availability may depend on the region.

This is the most challenging type of fraud to eliminate, due to the complexity of the mobile network system and the involvement of multiple operators. It is typically perpetuated by organized groups using illegal connections to direct a large volume of calls into high cost 'revenue share' service numbers, taking advantage of the roaming capabilities of SIM cards.

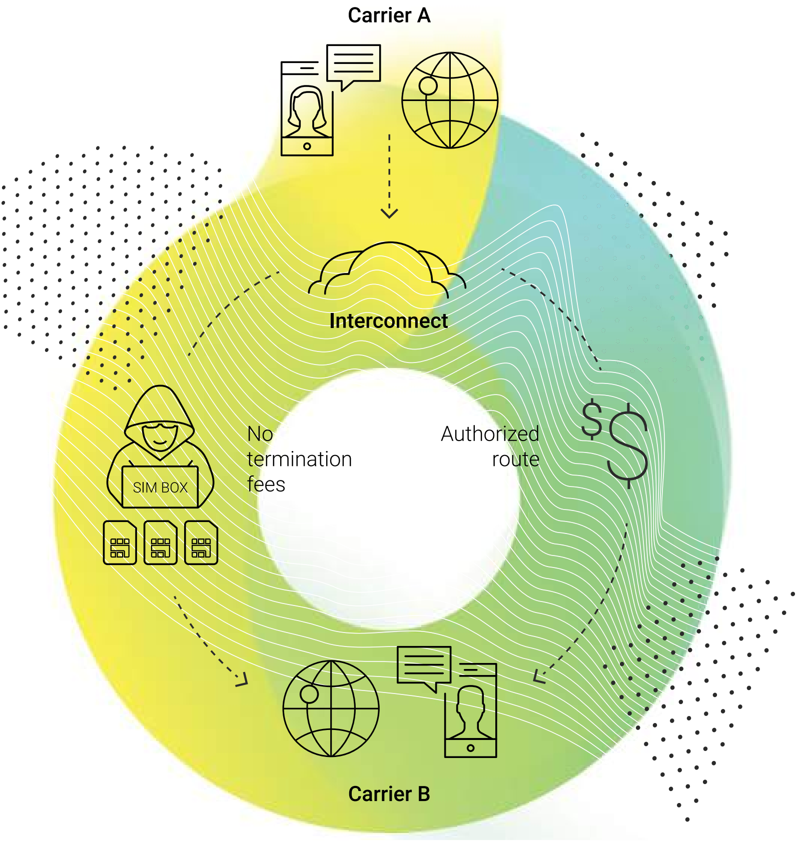
Wedo's experience shows that when there are no effective anti-fraud controls in place, sooner or later an operator will be hit by a major fraud problem. As the number of subscribers, distribution channels, and enhanced services grow, and more complex rate structures are put in place, an effective fraud management system is essential to minimize losses. RAID. Cloud exchanges data and voice records in near real-time, providing the detailed data required to detect complex yet subtle fraud patterns more quickly, allowing service providers to reduce the time it takes to detect fraud by 90% or more, helping to stop financial losses before they escalate.

How does our app work?



Bypass Fraud

Bypass fraud is one of the most common fraud types and it significantly affects operators, especially thos in developing markets where termination costs are higher.



There are several Bypass Fraud scenarios that should be monitored and the most common are:

Grey Routing

This is the arrangements that fall outside the regular course of business between the licensed telecoms companies in each country. The grey part of the route is usually realized at the far end where the call is terminated.

International Simple Resale

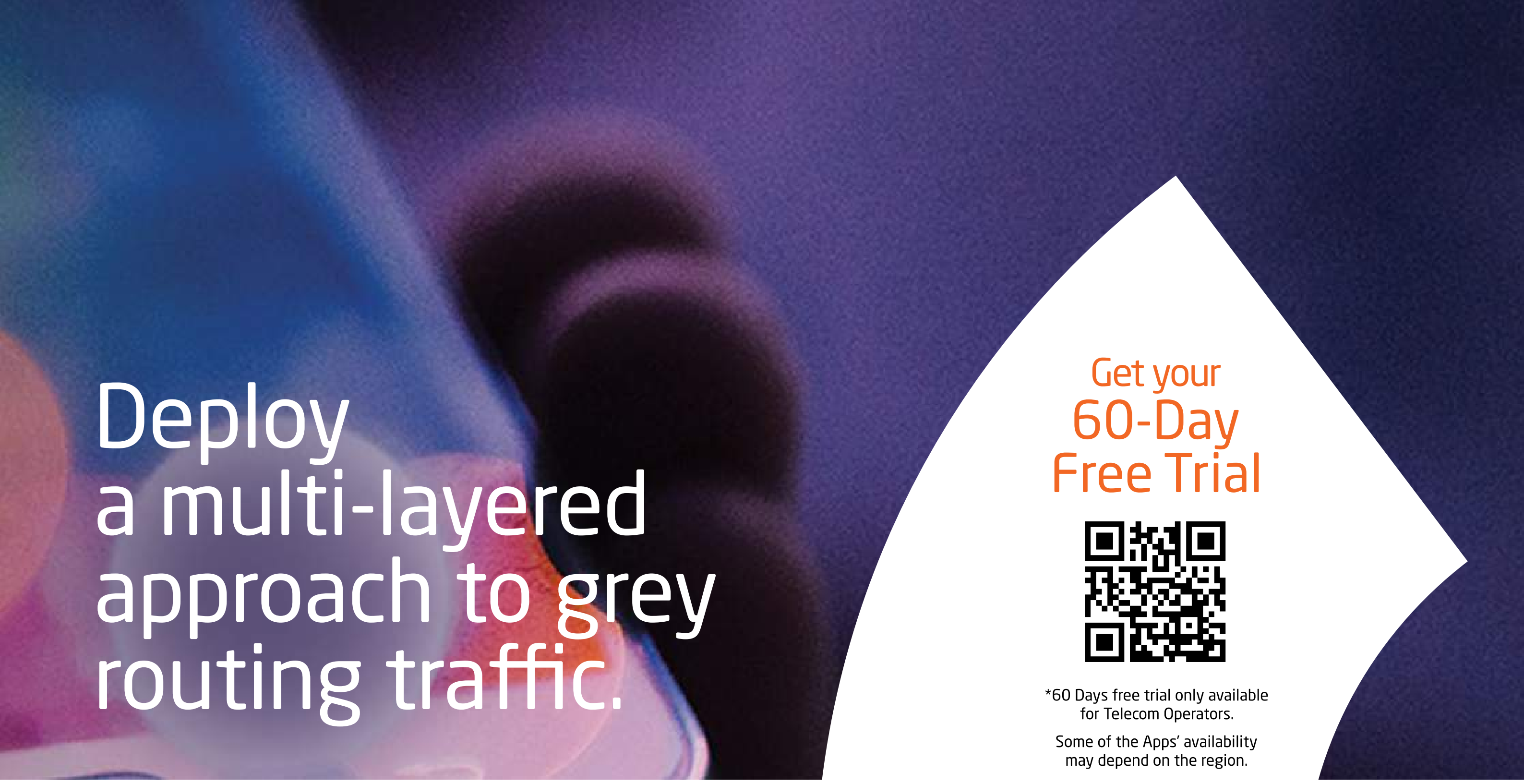
Involves landing off-net calls onto an operator's network but avoiding the international gateway to avoid the International interconnect charges.

Landing Fraud

Occurs when a call is "landed" on a carrier's network in a way that avoids toll charges. This is accomplished by making the traffic appear to have originated locally, or otherwise within the carrier's network.

SIM Boxes

Involves several SIM cards (pre or post-paid) used to generate many concurrent mobile calls.



Deploy a multi-layered approach to grey routing traffic.

Get your 60-Day Free Trial

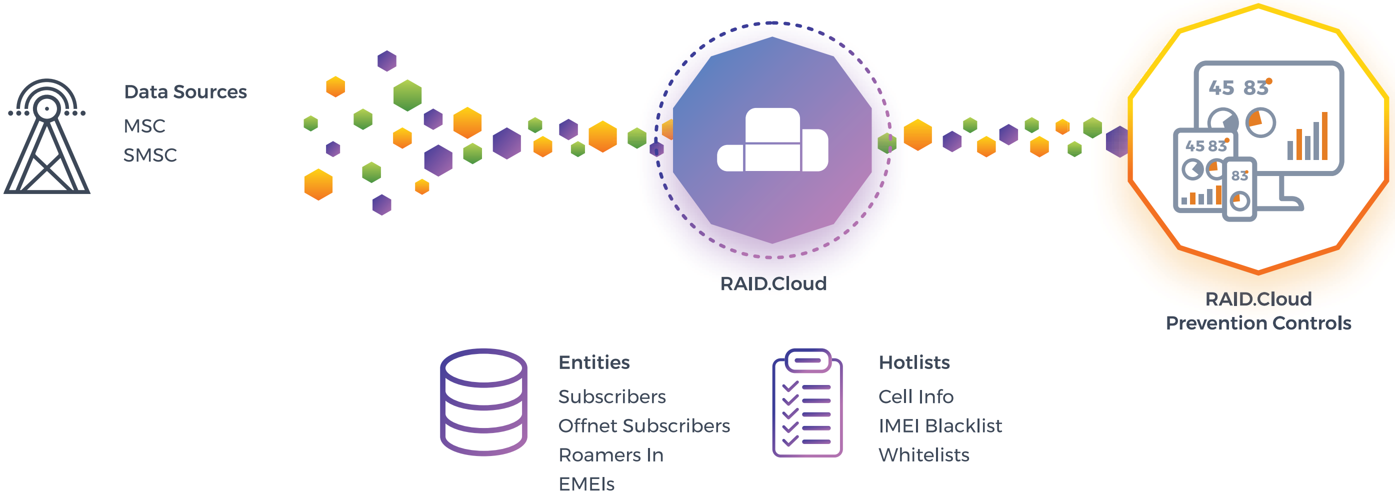
*60 Days free trial only available for Telecom Operators.

Some of the Apps' availability may depend on the region.

Bypass fraud is the exploitation of immobile to mobile gateway equipment, typically called SIM boxes, to hijack inbound international calls while transferring them over Voice over Internet Protocol (VoIP) to the mobile network. As a result of this action, it re-injects the call back into the mobile network, thus terminating as a local call at the destination, creating a divergence which makes the carrier operators lose their call termination charges.

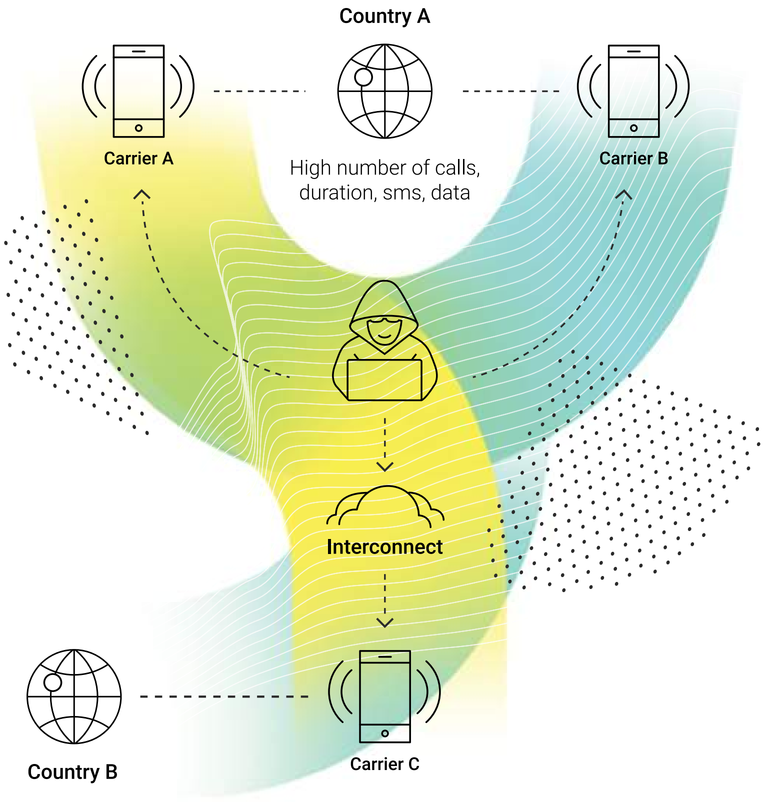
RAID.Cloud Bypass Fraud Application delivers an out-of-the-box solution to identify and recommend actions to stop these abnormal behaviors, delivering a service based on multiple layers of tracking, subscription-based access and security mechanisms to confirm Bypass Fraud MSISDN cases. Once detected, the application can then initiate a dedicated and combined analysis to uncover the associated numbers.

How does our app work?



High Usage Fraud

High usage scenarios can't be considered as a fraud scenario for the telecom operators. However, from the analysis of these scenarios it is possible to get some indicators, which when combined with others, can be useful in anticipating future fraud. These kinds of controls are already a huge help in monitoring service abuse by subscribers.



The high usage application will audit and control all the scenarios based on four main indicator groups:

On-Net Usage

Audit all the traffic, based on the CDRs generated at the network switches, to identify and alarm the scenarios where the traffic generated on-net is higher than a define threshold.

International Usage

Audit all the traffic, based on the CDRs generated at the network switches, to identify and alarm the scenarios where the traffic generated to international numbers is higher than a define threshold.

Off-Net National Usage

Audit all the traffic, based on the CDRs generated at the network switches, to identify and alarm the scenarios where the traffic generated off-net is higher than a define threshold.

Visitors Usage

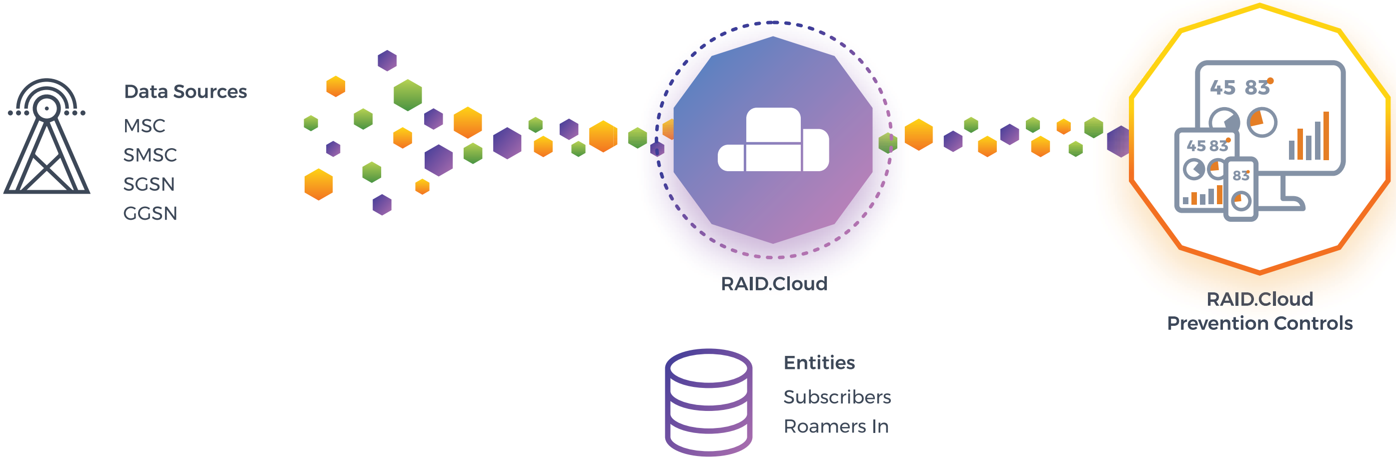
Audit all the traffic, based on the CDRs generated at the network switches, to identify and alarm the scenarios where the traffic generated by the roamer in is higher than a define threshold.

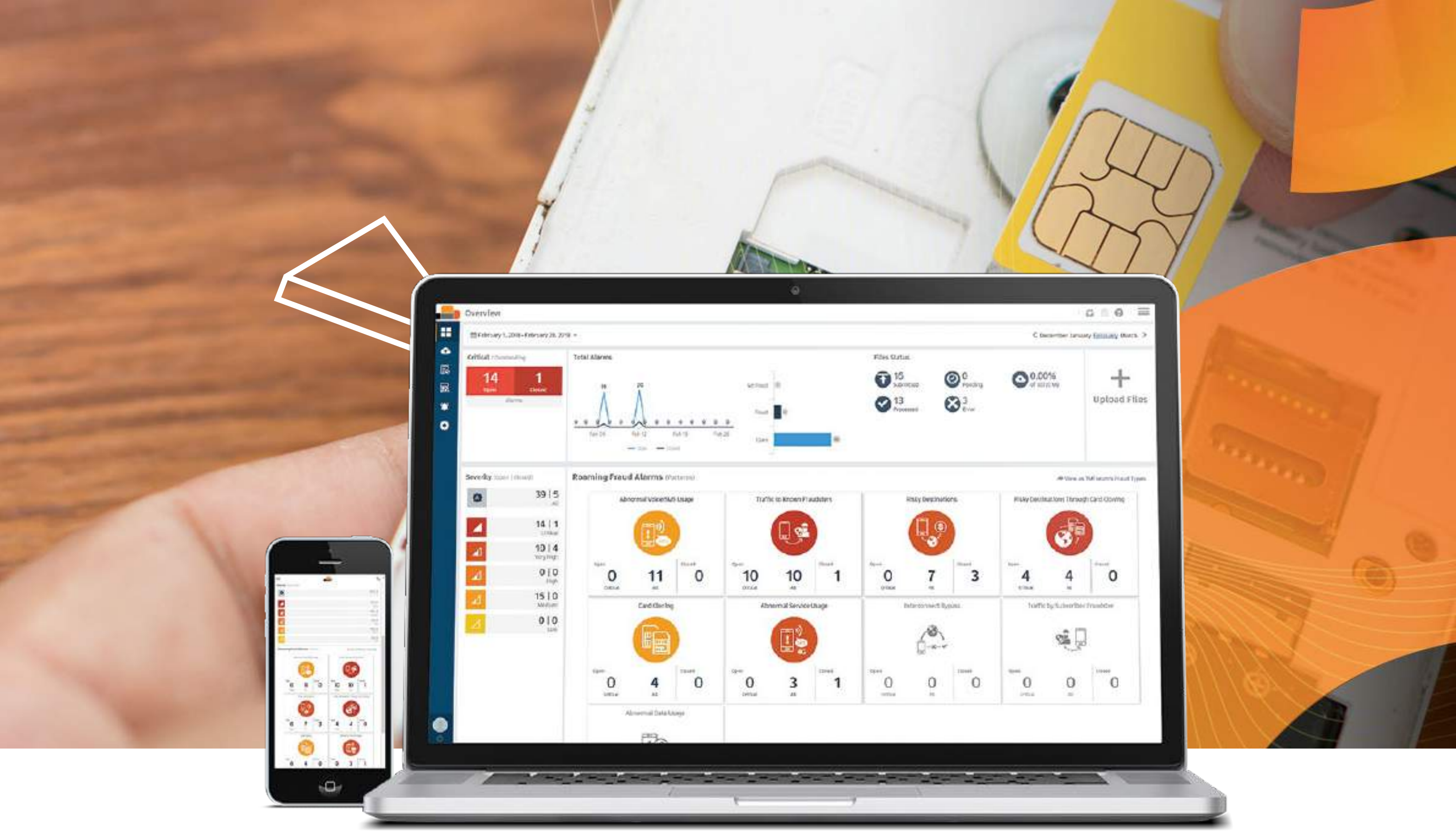
Anticipate fraud by monitoring your customers service usage.

The high usage application contains several engines and for each engine there are different rules that are used to identify possible fraudulent behaviors perpetrated by subscribers or inbound roamers. Each audited entity is classified according to a segmentation structure as defined in the solution. The segmentation determines the logical division of the entities into segments that may be used in detection or correlation in order to create more accurate rules focused on each segment level and value.

A set of detection flows are constantly running, aggregating and evaluating the rules thresholds defined by the fraud analyst. Once the defined traffic pattern thresholds are reached, alerts are raised. The data aggregation is done per actor (MSISDN, IMSI, or other) according to the segmentation and traffic under consideration. The data aggregation timeframe used to accumulate the relevant events is one day. The main purpose of this High Usage application is to check all the subscriber and roamer traffic and identify service abuse based on all on-net and off-net events. The records available are processed and aggregated using a 24 hour timeframe.

How
does our app work?





Prepaid Fraud

Prepaid fraud can have a huge impact in operators with a large prepaid subscriber's base due to the multiple actors that can be involved in those fraud scenarios, customers, employees, dealers and suppliers. This type of frauds often occurs from technical errors or system manipulation: IN, Voucher Management Systems (VMS), HLR, Billing among others.

There are several Prepaid Fraud scenarios that should be monitored and the most common are:

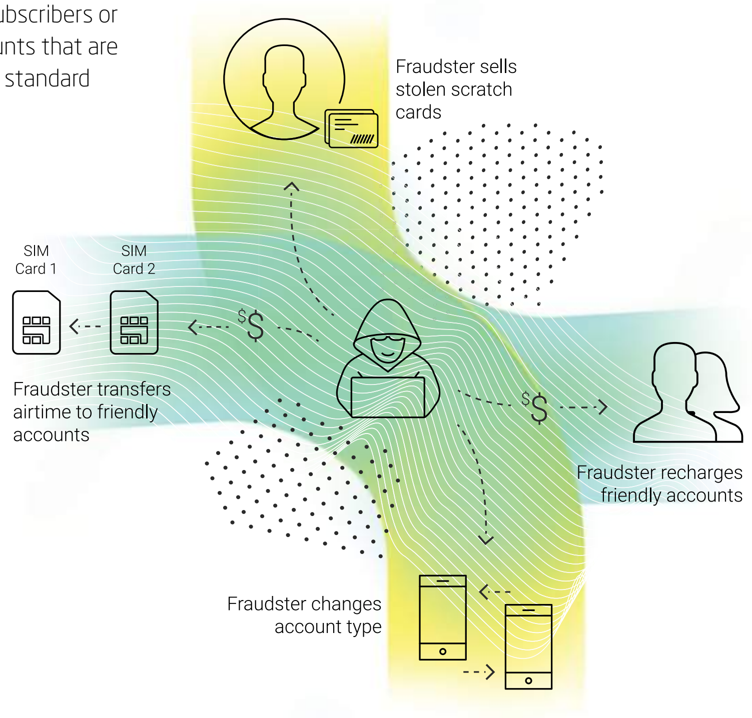
Stolen scratch cards to be sold in the market for your network with no payment collected

Manual recharges made internally to credit subscriber accounts without the corresponding payments

Airtime transfers to inactive subscribers or with amounts that are out of the standard patterns

Multiple account migration to take advantage of system inconsistencies to avoid paying for the traffic

Unauthorized or incorrect account balance adjustments


Fraudster sells stolen scratch cards
SIM Card 1
SIM Card 2
$
Fraudster transfers airtime to friendly accounts
$
Fraudster recharges friendly accounts
Fraudster changes account type

Protect your business from prepaid account manipulation stopping fraudsters from illegally modifying account balances and account types

Get your
60-Day
Free Trial

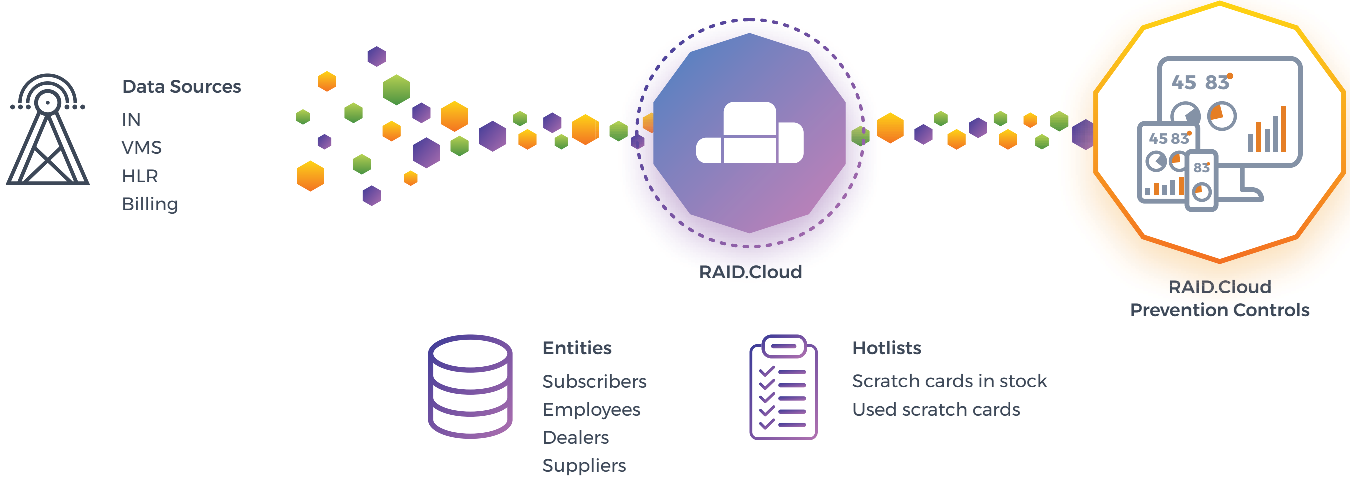
*60 Days free trial only available for Telecom Operators.

Some of the Apps' availability may depend on the region.

CSPs can deploy various defence mechanisms to mitigate against losses and ensure fast detection by ensuring processes are continually reviewed, staff are educated in new fraud trends, new products and services are assessed for fraud and security weaknesses and state of the art technology is used to quickly raise alerts for suspect activity.

Fraud management can be a time consuming and overwhelming activity especially for those CSPs who are not yet mature in the development of fraud control and prevention strategies. RAID. Cloud is able to support CSPs in this space, to review, advise upon and implement fraud management strategies, train fraud personnel, deliver and optimise fraud management systems or deliver the complete fraud management process in minutes.

How
does our app work?



Data Sources
IN
VMS
HLR
Billing

RAID.Cloud

RAID.Cloud
Prevention Controls

Entities
Subscribers
Employees
Dealers
Suppliers

Hotlists
Scratch cards in stock
Used scratch cards

Subscription Fraud

Subscription fraud involves obtaining customer information required for signing up to a new telecommunication contract or service with a valid authorization but without any intention to pay for the products and services used.

The theft here is plain and simple but it's hard to detect 'intent' at the point of sale. This is the starting point for many other telecoms fraud scams and as such is recognized as the most damaging of all non-technical fraud types.

Perpetrators don't just stop with obtaining legitimate service illegitimately, they usually use it as a precursor to other types of fraud such as Premium Rate Fraud and International Revenue Share Fraud, which are lethal in their own right.

The real impact of this type of fraud is difficult to measure because it does not stop with revenue loss alone. The effects can be catastrophic in terms of escalating complaints, poor customer experience, dissatisfaction among support staff, and diminishing investor confidence.

The possible fraud scenarios that can be perpetrated are:

International Revenue Share Fraud

Interconnecting payments for calls in roaming or off-net made using services or equipment's obtained with false subscription data.

Commissions Fraud

Dealers can gain commissions by simulating false services or equipment sales.

Service Reselling

Fraudsters sell service to other customers at below market rates as no payment is going to be made to the service provider.

Premium Rate Service Fraud

Fraudsters commit PRS calls and operators find it impossible to collect the amount spent.

Assets acquisition

Buying new equipment or services with a retention agreement with no intention to pay.

Make subscriber identity trust decisions with confidence

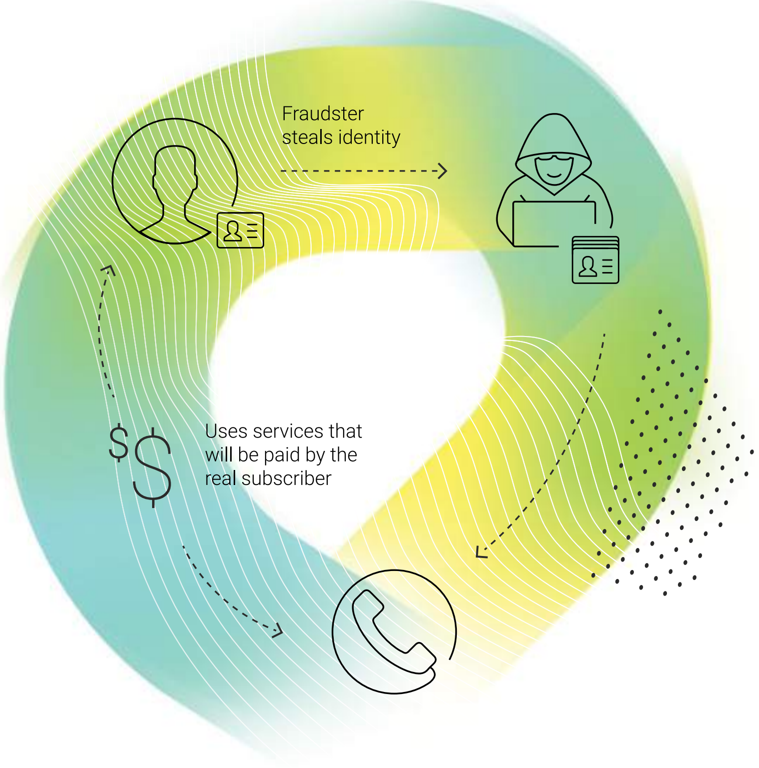
Get your
60-Day
Free Trial

*60 Days free trial only available for Telecom Operators.

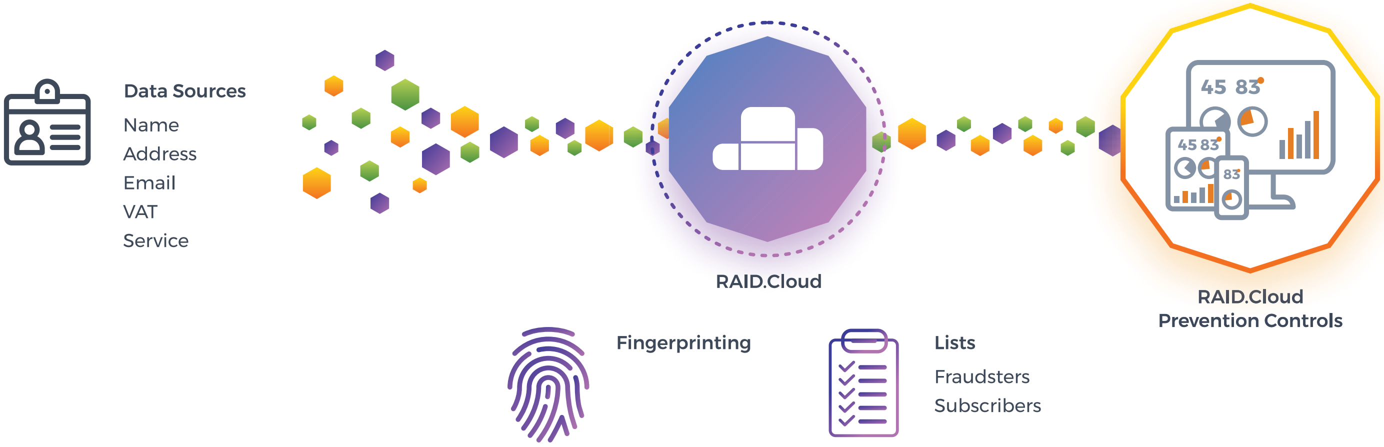
Some of the Apps' availability may depend on the region.

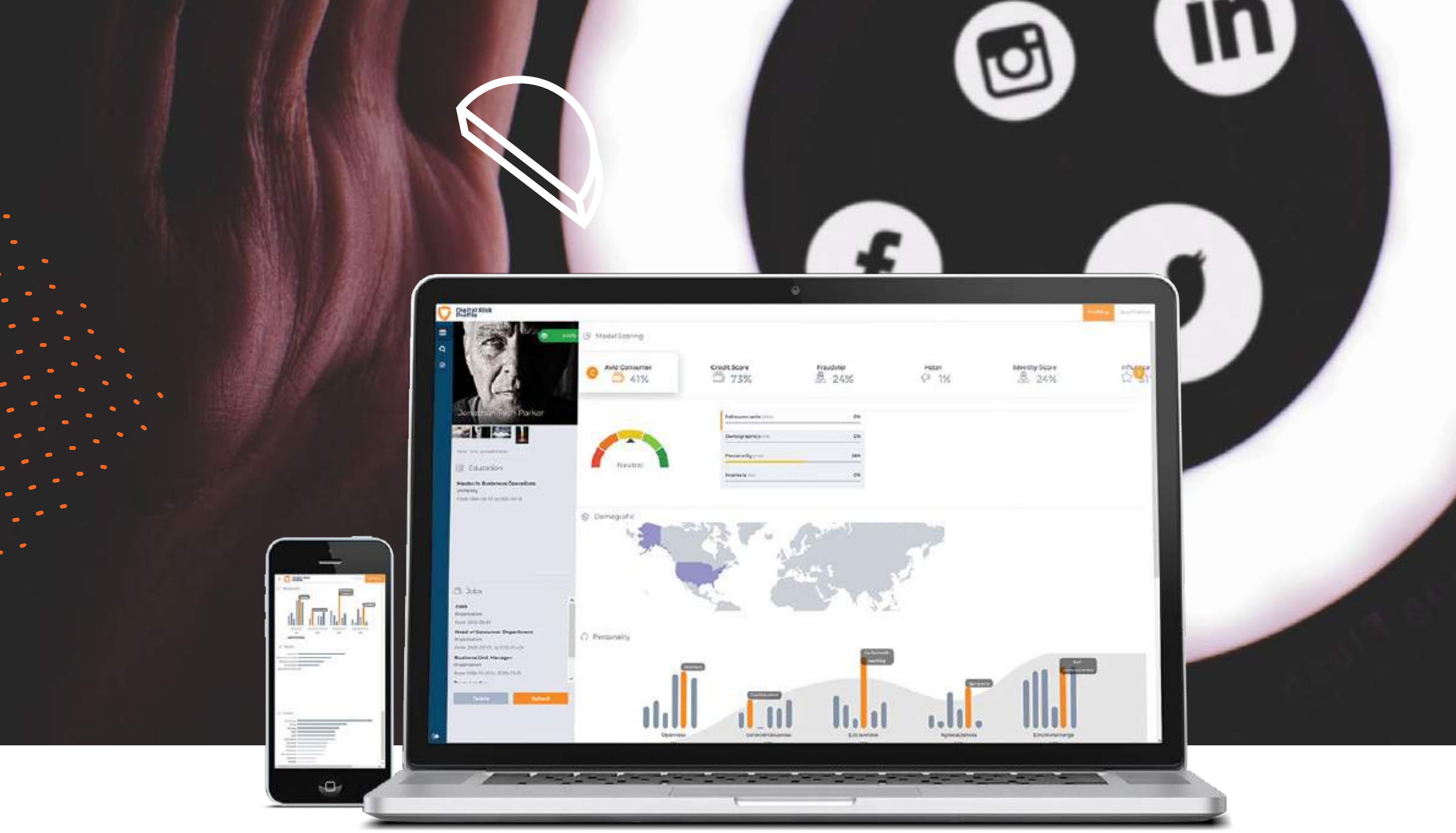
Subscription fraud is often categorized as bad debt rather than fraud. Operators globally estimate that nearly 40% of all bad debts are actually subscription fraud. RAID.Cloud Subscription Fraud app is designed to monitor and detect new attempts to re-enter the network.

The engines evaluate new subscribers for instances of multiple activations and then using fingerprinting through social networks, can identify and classify fraudulent activities when they occur in near real time.



How
does our app work?





Digital Risk Profile

The growing quantity and complexity of digital data available offers the chance to harvest threatening data from the web, IRC channels, forums, paste sites, social media, and threat feeds.. But attempting to find and collate this information manually is as inefficient as it is cost intensive.

Digital Risk Profile application crawls the web in real-time to gather information, the main goal being to provide a subjective understanding of an entity (customer, partner, company...) represented as indicators related to behavior, activities, subscriptions and related content. Threat actors have moved beyond their traditional stomping grounds of web and email to exploit the riches of new digital territories, in particular, social media platforms, and organizations' digital trails are typically larger and more complex than those of an individual.

The ability to create a digital DNA of individuals and their distinctive online footprint together with trusted digital identities that fraudsters can't fake makes fraudulent behavior far easier to detect, as the Digital Risk Profile of a fraudster is significantly different from a trusted user.

The integration of Digital Risk Profile's collected information with line-of-business applications allow you to:

Exploit relevant information from customers to align go-to-market strategies and company offers.

Provide customers with information about data protection and leakage through conditional opt-in based rewards programs.

Assess your customer's profile and map different sorts of behavior.

Discover compromised information.

Evaluate Third Party Vendor data based on online discussions.

Make digital authentication and authorization strict for cybercriminals but seamlessly for trusted subscribers.

Get your
60-Day
Free Trial

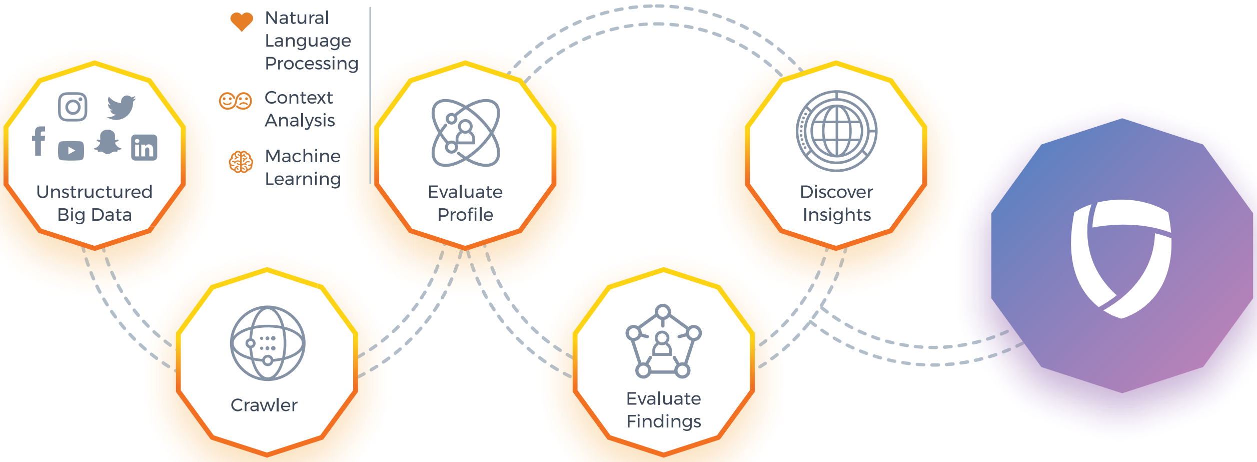
*60 Days free trial only available for Telecom Operators.

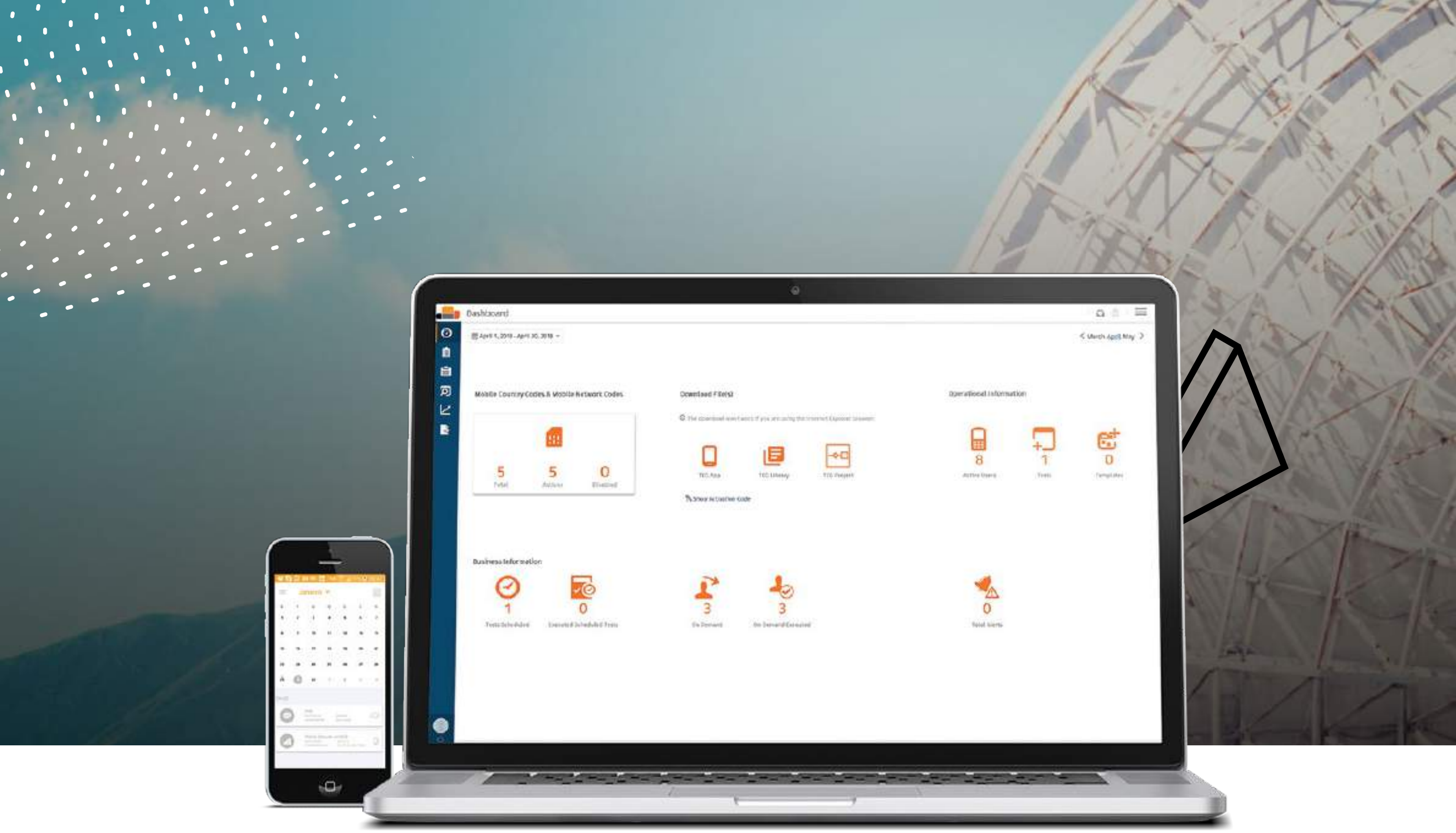
Some of the Apps' availability may depend on the region.

This flexibility allows you to add extra value and enhance your line of business solutions with real-time assessment to qualify customers, prospects & companies, identify information to enhance & develop marketing campaigns, and drive company strategy recognizing market trends and liabilities to better focus services and offer.

Digital Risk Profile application combines scalable data analytics with machine learning roles analysis to monitor for cyber threats, data leakage & reputational risks, an, to create an up-to-the minute views of an organization or individual through public online sources.

How
does our app work?





Service Assurance

In today's networks, delivering superior customer experience and service quality depends on too any variables. CSPs often risk service quality without adequate testing which results in high maintenance costs and increased chances of failure and customer dissatisfaction.

RAID.Cloud Service Assurance app allows CSPs across the globe to meet their network testing requirements by leveraging social crowding to reduce time and effort in testing service quality and reliability. As applications are more widely distributed and require more bandwidth, networks grow and become more complex; and at the same time multiple applications running on smartphones now with the explosion in consumption impact on the quality perceived by end user.

Service Assurance app data collection is based on crowdsourcing and gamification reward programs. There is no survey required, just user consent for an application to run and collect information to analyze service performance. This allows CSPs to collect and analyze data in a central cloud repository about service quality and reliability using regular smartphones.

The application allows for the definition of custom time triggers for real-time testing of multiple call and data services, thus assuring the overall performance of the network (QoS) and the customer experience while using the provided services (QoE).

Leverage crowd-sourced data to reduce time and effort by testing QoE & QoS.

Get your
60-Day
Free Trial

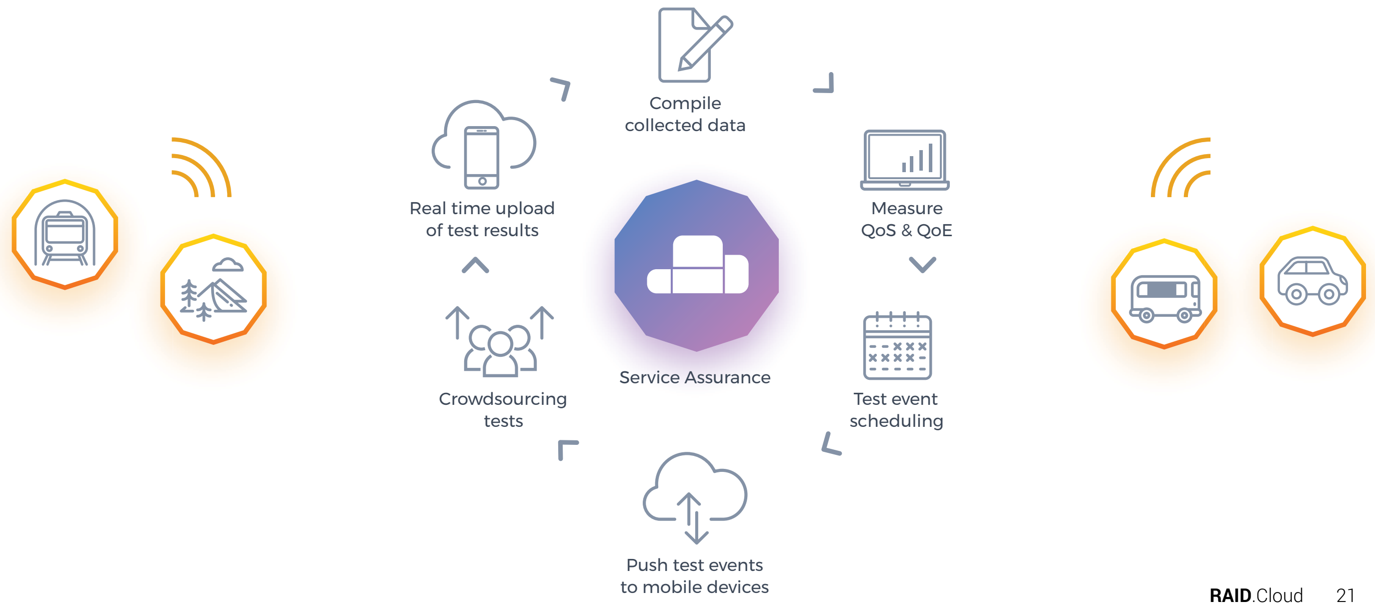
*60 Days free trial only available for Telecom Operators.

Some of the Apps' availability may depend on the region.

RAID.Cloud Service Assurance is a distributed test platform for mobile communications providers, making use of the cloud and the growing computing power of smartphones to: drive tests, prevent revenue leakages & fraud, monitor network performance and gather device & application analytics.

Our solution is based on two components - one central console to create, evaluate, schedule and analyze the out coming of the tests, and an android application to execute the tests while smartphones are idle, leveraging the growing computing power of these devices. This can be used by your workforce, or even your own customers, to help you to enhance your offer to the market

How
does our app work?



Managed Services

EXTENDING SKILLS TOGETHER
WITH YOU AND YOUR TEAM.

RAID.CLOUD TRIAL

Think you will be abandoned during the trial period?
Think again.

WEDO believes the best way to prove the value of our applications is to allow you to trial the solution with no feature limitations.

We allow you to use our applications for 60 days, so that you can collect insightful information about what is happening on your network when it comes to fraud threats.

We support you through the trial process by sitting down with you to evaluate initial findings and then helping you to customize the app's thresholds to increase detection accuracy. Don't worry about data transformation and integration either. We also work with you to get your data correctly formatted and processed by our cloud applications.

It's as simple as **REGISTER & GO**

RAID.CLOUD STANDARD

Continuously monitor the health of your RAID.Cloud
Applications to proactively detect alarms and notify analysts.

RAID.Cloud Standard Services provide you with full autonomy in using our fraud management apps. As a part of this subscription level, WEDO provides initial support to you when processing data for the first time, with ongoing help for increasing fraud detection accuracy, making adjustments and training.

Our dedicated support team is composed of experienced technicians each with a minimum of five years of experience in fraud management and all certified in RAID.Cloud Apps. They are there to ensure you get best service possible.

RAID.CLOUD PRO

Enjoy the all the best from the cloud with the trust of an expert.

Tackling fraud can be a time-consuming task for your team. With PRO services, WEDO aims to deliver added value services to you with two main objectives:

1) Reduce costs and time for internal fraud teams in understanding what is happening in your network and which actions to take.

2) Share our fraud expertise gathered from projects from all over the world with your team.

With this subscription level, you'll have access to a team of our fraud experts who will monitor your data and have regular follow-ups with your assigned team to enhance results and provide the best security possible to your network.

RAID.CLOUD PREMIUM

Expert Fraud Management staff in a transformational model built to deliver qualitative results.

Companies more than ever need to focus on their core business so RAID.Cloud Premium Services are designed to provide you with full fraud support. With a focus on operational transparency, we supply you with a dedicated team of fraud and network specialists to monitor your network and adjust the apps according to your specific network reality.

We manage the apps, customize the thresholds & hotlists, deliver activity reports, and recommend mitigation actions in order to keep your network secure.

Stay constantly updated and alerted on what is happening with the support of our team..

Let us be part of your team.

WeDo Technologies,

founded in 2001, is the market leader in Revenue Assurance and Fraud Management software solutions to Telecom, Media and Technology organizations worldwide.

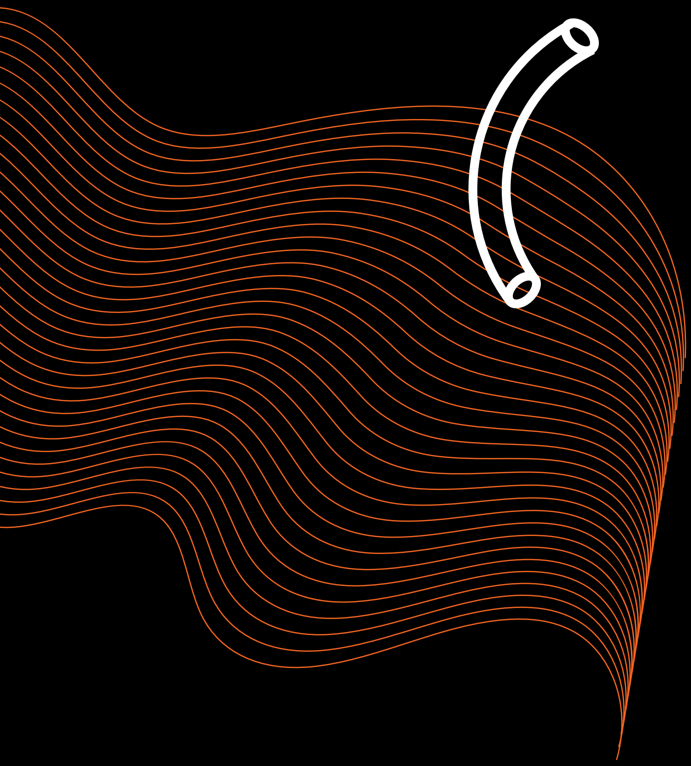
WeDo Technologies provides software and expert consultancy across +105 countries, through a +600 network of highly skilled professional experts, present in the US, Europe, Asia-Pacific, Middle East, Africa, Central and South America.

WeDo Technologies' software analyzes large quantities of data allowing to monitor, control, manage and optimize processes, ensuring revenue protection and risk mitigation.

With over 180 customers - including some of the world's leading blue chip companies - WeDo Technologies has long been recognized as the constant innovator in assuring the success of its customers along a journey of continuous transformation.

Offices

Portugal
Brazil
Egypt
France
Ireland
Malaysia
Mexico
Spain
UK
USA



FOLLOW US!

WeDo Technologies
@WeDoNews
@WeDoposts
WeDo Technologies
WeDo Technologies
WeDo Technologies
www.wedotechnologies.com

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional

Know the unknown