SANDVINE

Data Fraud Management

Get paid fairly by detecting and mitigating a range of zero-rating fraud techniques

DATA FRAUD MANAGEMENT DELIVERS:

Zero-Rating Fraud Prevention
Detects and prevents attempted fraud leveraging zero-rating exploits

Prevention of Unauthorized Access
Restricts specific applications that are not allowed with certain plans or by regulatory restrictions

Terms and Conditions Fraud Prevention
Blocks attempted circumvention of terms and conditions that can lead to network abuse (e.g., tethering or line sharing)

MARKET OVERVIEW

Network operators are challenged with attracting new users and improving the trend of declining ARPU. In order to solve these problems and grow market share in a fiercely competitive landscape, operators must innovate their service offerings to gain new customers and retain existing ones.

One popular tool is zero-rating, as it allows operators to achieve market differentiation and offer value to attract new users, as well as retain existing ones. However, the use of zero-rating creates a new and attractive surface for unscrupulous users wanting to exploit weaknesses in the network and bypass payment for the services offered, which directly impacts the operators' revenue and the brand perception.

To successfully implement zero-rating, operators need to be aware of the cost of zero-rating – fraud – and apply careful planning and market awareness to ensure they get paid for the services they deliver. Specifically, operators need to be able to detect and act to prevent various methods of zero-rated fraud. Misclassification of traffic and unmanaged fraudulent behavior can have heavy financial consequences due to charging errors, unnecessary capacity expansions, and deteriorating quality of experience for regular users.

There are a variety of techniques used in zero-rated fraud, such as HTTP header injection, domain fronting, and DNS spoofing, but data fraud is not limited to zero-rating.

Additional target areas for fraud:

- Subscription mismatch between IT and network (e.g., prepaid subscriber connecting as postpaid)
- Abuse of commercial terms and conditions for plans (e.g., tethering restriction)
- Billing charges for events (e.g., ringtones or music on demand)
- Access to unauthorized content
- Regulatory compliance (e.g., child pornography restrictions)

The challenge for operators is not isolated to only detecting fraudulent behavior, but also taking the right action and preventing abusive usage, not only targeting zero-rating practices, but in the network overall to protect valuable revenue.

Sandvine's frequently updated signature library ensures accurate identification of attempted data fraud and enables active management to prevent fraud

Data Fraud Management Lifecycle

1 Analyze & Deep-Dive

Identify suspicious traffic and subscribers and understand the underlying protocol usage and behaviour through deep-dive

2 Isolate

Segregate the traffic and subscribers from regular traffic

3 Build Signature

Create a custom signature to detect suspicious traffic

4 Take Action

Apply blocking, shaping, or reporting action

SOLUTION OVERVIEW

Sandvine's Data Fraud Management solution uses the ANI Classification Engine to deliver superior traffic classification and policy enforcement to strengthen operators' defense towards fraudulent behavior in the network. The right policy enforcement empowers the right response to fraud when detected and, with behavioral analysis, heuristics, and machine learning, prevent future fraud as well as potentially recover lost revenue even if the traffic is encrypted.

Sandvine has partnerships with OTT application providers to ensure that traffic associated with these applications is classified correctly through the Sandvine Gateway API. In the case of sponsored data opportunities, this API has the ability to build trust between operators and content owners, minimizing billing errors. With correct classification and billing, operators can confidently implement zero-rating and take advantage of sponsored data opportunities as they can mitigate revenue loss associated with fraud, misclassification, or billing errors.

Sandvine's Data Fraud Management delivers these key capabilities to any zero-rating data practice:

- Advanced traffic classification powered by machine learning, heuristics, and behavioral analysis, to deliver accurate application and traffic identification, even for encrypted traffic
- Rich policy enforcement options to empower network operators to respond appropriately when fraud is detected, prevent fraud, and potentially recover lost revenue
- Advanced reporting and analytics that provide insight into the prevalence of data fraud and the impact of management policies
- Sandvine Gateway API for partnerships with OTT and application providers for ensuring accurate traffic identification for high-profile OTT traffic

Sandvine's rich visibility and reporting visualization ensures that the operator can see the scope of the fraud that is occurring on their network, and then determine the appropriate actions to take, including drilling down to determine the exact techniques being attempted to commit data fraud.

Data Fraud Management enables operators to detect and act on fraudulent behavior occurring inside the network. With traffic visibility, fraudulent users that have abused service agreements can be moved to a higher volume plan and charged for their usage, and operators can recover valuable revenue.

ABOUT SANDVINE

Sandvine helps organizations run world-class networks with Active Network Intelligence, leveraging machine learning analytics and closed-loop automation to identify and adapt to network behavior in real-time. With Sandvine, organizations have the power of a highly automated platform from a single vendor that delivers a deep understanding of their network data to drive faster, better decisions. For more information, visit **sandvine.com** or follow Sandvine on Twitter at **@Sandvine.**

SANDVINE

USA
2055 Junction Avenue
Suite Number 105
San Jose,
CA, 95131
USA

EUROPE
Svärdfiskgatan 4
432 40 Varberg,
Halland
Sweden
T. +46 340.48 38 00

CANADA
408 Albert Street,
Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
RMZ Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333