SOLUTION BRIEF

SANDVINE

Data Revenue Leakage Monitoring

Identify misconfigurations and oversights that cause revenue loss

DATA REVENUE LEAKAGE MONITORING DELIVERS:

CDR Validation
Ensures that CDRs are accurately accounting for all network traffic from users

Incorrect User Configuration Detection
Identifies incorrect network configurations where usage records do not match the expected usage profile

Complex Service Plan Validation
Validates correct usage by plan is being billed, which is critical when dealing with complex plans, such as application- or content-based charging

MARKET OVERVIEW

As operators battle profitability issues, declining ARPU, and increasing network costs, they are developing new and innovative service plans to keep up with their competition and increase customer satisfaction. However, innovative service plans increase the risk for revenue leakage and will have serious financial consequences for operators.

Users are drawn to specialized data packages that are tailored to their usage patterns and where they can get more value from their service plan, such as zero-rated offerings and personalized services. With the number and increasing complexity of service plans, delivering the best services creates more charging system risks.

This complexity goes beyond service plans and occurs across the rest of the network. Revenue leakage is a multi-faceted problem and can often also be caused by the complications of running multi-vendor environments. With multiple network elements working together to deliver better performance and more satisfying services, the risk of functional deficiencies is greater, and software upgrades can cause unanticipated complications, and can therefore go undetected. These types of revenue leakage may be innocent in nature compared to fraud, but can have a large financial impact for operators who are already suffering from profitability issues.

To mitigate leakage-related issues, some operators have launched designated teams tasked with revenue assurance, which entails identifying incorrect billing and ensuring a billing backup by independently generating, collecting, and reconciling CDRs. An effective revenue leakage solution requires accurate traffic classification and counting to minimize billing errors and leakage. It also provides revenue assurance teams the ability to detect misconfigurations in a timely manner and guide other teams on what analytics to collect and how to discover abnormalities.

SOLUTION OVERVIEW

Sandvine's Data Revenue Leakage Monitoring solution provides operators an additional set of eyes in the network to accurately measure usage, classify traffic, and detect problems in the control and charging planes. For a revenue assurance team, this solution can work as a point of comparison for other systems, and serve as a fallback measure that preserves charging capabilities in the event of a service outage for other usage collection systems.

The ANI Classification Engine ensures accurate identification of data revenue leakage for application-based plans

This solution leverages advanced traffic detection and classification techniques, and accurate and comprehensive data usage reporting. It also has built-in service plan validation for ensuring that users with top-tier or high-value plans are billed correctly for their usage. Usage is reported in multiple standard formats to deliver an effective revenue assurance solution, saving money because Sandvine's resilient CDR collection solution removes the need for redundant CDR solutions.

Sandvine's Professional Services team provides continuous management of policies, signatures, and techniques, and also provides valuable insights through reporting to meet the challenges of the complex and ever-changing network environments of modern operators.

Through this comprehensive solution offering, Sandvine minimizes the impact of network misconfigurations and outage-related events that result in revenue leakage. Operators implementing this solution can not only recover their lost revenue, but also pursue other revenue-generating opportunities without the risk of leakage. By providing the right data to swiftly identify the causes of leakage, Sandvine employs preventative measures and checkpoints to identify and stop leakages and preserve valuable revenue for operators.

Figure 1

Data revenue leakage monitoring potential for service plans

Service Plan	Potential for Revenue Leakage	Notes
Tiered Plans	Medium to High	Non-real-time CDRs risk leakage
Roaming	High	Incorrect data accounting when transit providers still need to be paid
Tethering	Medium to High	Multiple PDP contexts and faulty tethering detection
Application-Based Plans	High	Misclassification of traffic due to changes

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

This documentation, including all documentation incorporated by reference herein such as documentation provided or made available on the Sandvine website, are provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Sandvine Corporation and its affiliated companies ("Sandvine"), and Sandvine assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect Sandvine proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of Sandvine technology in generalized terms. Sandvine reserves the right to periodically change information that is contained in this documentation; however, Sandvine makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.