SANDVINE

Regulatory VoIP Management
Manage illegal or unlicensed VoIP

REGULATORY VOIP MANAGEMENT DELIVERS:

Industry-Leading Signature Library
Recognizes all VoIP applications via an industry-leading signature

Machine Learning-Powered Advanced Classification
Identifies encrypted traffic through sophisticated heuristics powered by machine learning

Circumvention Technique Detection
Detects sophisticated techniques used to circumvent regulations, including tunnelling and masquerading

Revenue Protection
Protects critical voice revenue for operators with a high return on investment

MARKET OVERVIEW

The use of operator-provided voice services has decreased over the past few years with specialized VoIP-applications entering the communication space. Today, there are several different ways to make a voice call without actually dialing a phone number. These applications often have both voice and messaging services available and use heavy encryption to protect user privacy.

For operators, this change to application-based voice services means losing previously earned revenue. However, in some regions, operators are allowed to block the use of VoIP applications to protect their revenue and, in others, government regulators are concerned with the safety and security aspect posed by these encrypted communication channels.

Many VoIP applications also offer direct messaging and, with increasing use of encryption, it is critical to be able to identify these applications to address the potential security concerns. Since encrypted VoIP applications are among the most sophisticated and aggressive in attempting to avoid detection, managing this traffic is one of the biggest technology challenges for regulated operators. Providers of these VoIP applications have no obligation to adhere to local laws and the responsibility to uphold a jurisdiction's regulations, permitting only lawful voice and messaging services, falls on the operator.

By regulating OTT-VoIP applications, possible unlawful communication can be steered to compliant voice-services that adhere to governmental laws regarding cooperation with Law Enforcement Agencies.

Figure 1

Overview of Regulatory VoIP Management in the ANI Portal
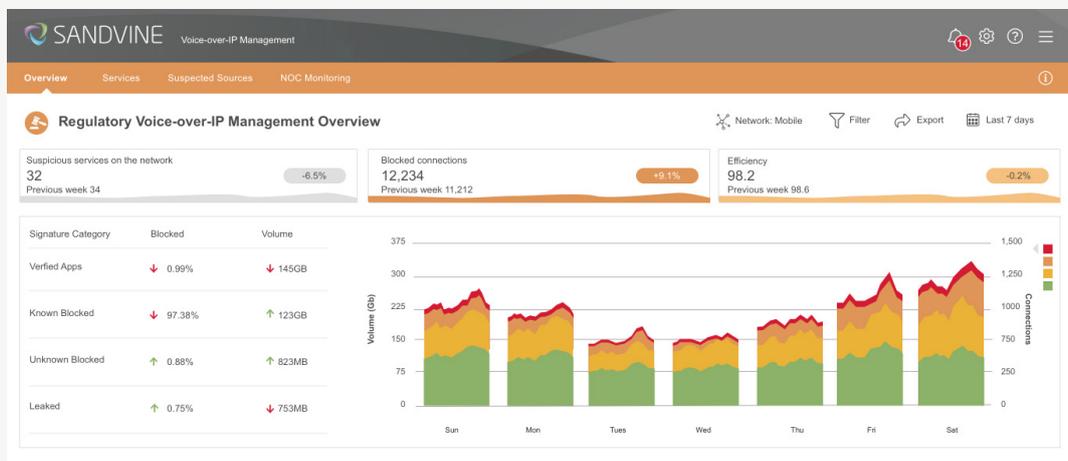
Active Network Intelligence delivers the most efficient VoIP management solution on the market

SOLUTION OVERVIEW

Sandvine is the leader in identifying traffic – especially encrypted traffic. Regulatory VoIP Management leverages the ANI Classification Engine to correctly identify VoIP applications and provide the broad functionality and flexibility needed to deliver reliable compliance, while also preserving the ability to adapt to changing regulations, traffic makeup, and usage patterns.

ANI Classification Engine

The foundation of Sandvine's Regulatory VoIP Management solution is the ANI Classification Engine, which supports hundreds of VoIP application signatures and protocols, including encrypted applications. With frequent updates, operators can comply with confidence even as new and existing applications get introduced and updated. Operators also have the option to design their own custom signatures if they are offering alternatively managed VoIP services.

Action-Based Capabilities

Once VoIP traffic is identified by the ANI Classification Engine, multiple actions can be applied to comply with regulations. For instance, unlicensed VoIP traffic can be blocked or rejected, which will prevent calls from connecting; alternatively, traffic can be rate-limited or session-limited, which delivers more effective results for some types of VoIP applications (e.g., polymorphic applications that change behavior when blocked).

If logging or analytics is part of the regulatory requirement, then statistics can be gathered on VoIP traffic passed, blocked, limited, or dropped; these statistics include volume, number of call attempts, quality of experience, and many other metrics that provide a closed-loop analysis of the overall compliance effectiveness.

Regulatory VoIP Management can be integrated with policy systems to provide more information regarding usage patterns to further narrow down the blocking policies. For example, if some users are allowed to use specific VoIP applications as part of a corporate plan, their traffic can be allowed to pass. This integration provides operators and regulators with increased customization capabilities as well as flexibility when enforcing compliance regulations.

Sandvine's solution can be deployed anywhere in the network – on a virtual CPE, provider edge, core, or peering point. When deploying Regulatory VoIP Management, Sandvine is traditionally placed inline, enabling the solution to natively block traffic that is deemed to be non-compliant with the VoIP regulations in place.

Figure 2

Regulatory VoIP Management Deployment Diagram
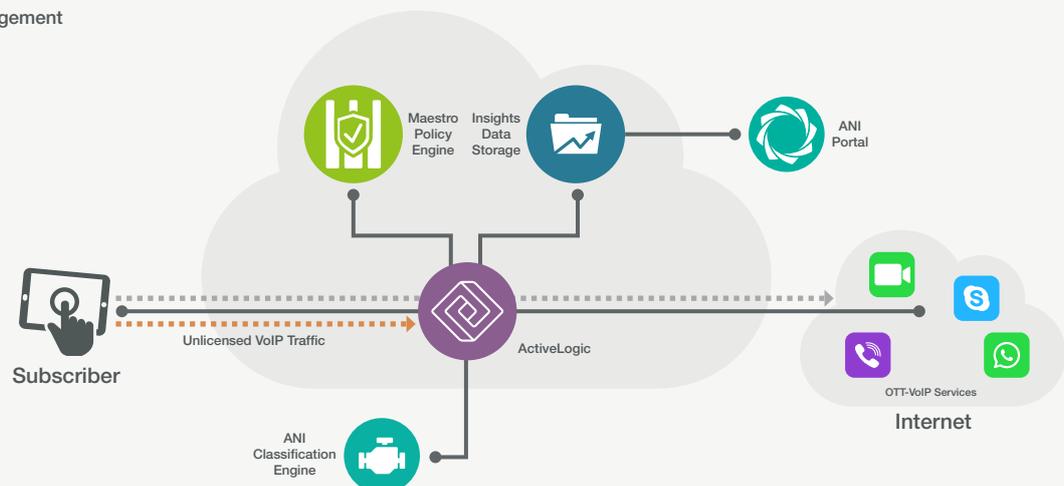
Regulatory VoIP Management leverages Sandvine's unique Active Network Intelligence, combining leading application identification with unparalleled traffic management precision to deliver the most effective VoIP management solution.

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.**

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

SANDVINE.COM