



KEY BENEFITS

- Provides device-related insights for sales and marketing to create compelling targeted offers
- Gives real-time, contextual intelligence, critical for running and optimizing networks and ensuring good QoE
- Enhances existing use cases with augmented data, which is updated frequently for accuracy and coverage
- Simplifies management with a dedicated framework
- Empowers the Cyber Threat Analysis and Cyber Threat Management use cases to offer enhanced subscriber protection

iFeeds

Sandvine's real-time contextual intelligence feeds

Access or data volume has never been an obstacle for operators. In fact, the issue has always revolved around the relevance, accuracy, and usefulness of data. As networks evolve to new architectures for 5G and cloud deployments, increasing the context of data becomes more critical to make intelligence actionable. With the adoption of more devices, applications, and access types, the need for clear visibility and understanding is imperative to determine the root cause of network congestion, quality, or security issues.

However, many solutions cannot deliver the required context or insights in real time, instead performing this analysis after the fact, rendering them less effective in helping operators confidently make business and network decisions. It also drastically limits the effectiveness of any automation strategy, which requires this information to be constantly available for policy updates.

As a network intelligence leader, Sandvine arms operators with the visibility and contextual awareness required to run world-class networks. Sandvine's Application and Network Intelligence (ANI) product portfolio enhances application QoE and network intelligence use cases for operators, making them superior by adding real-time actionable intelligence and relevant context including application, device, and location to basic network statistics.

INTELLIGENT FEEDS (iFEEDS)

Sandvine's award-winning ActiveLogic data plane classifies all application traffic. As part of this process, Sandvine can leverage a set of iFeeds to augment and correlate the data with additional actionable attributes. These feeds can be added in real time to drive additional analytics, traffic management, and charging context, enhancing a variety of ANI use cases.

iFeeds is a collection of different data feeds that are integrated into the ANI Classification Engine to deliver a single visibility and enforcement point (**Figure 1**). Each feed has a distinct function and is examined as part of the Sandvine's classification process based on the individual use case requirements (**Table 1**).

iFEEDS DATABASES

ContentLogic

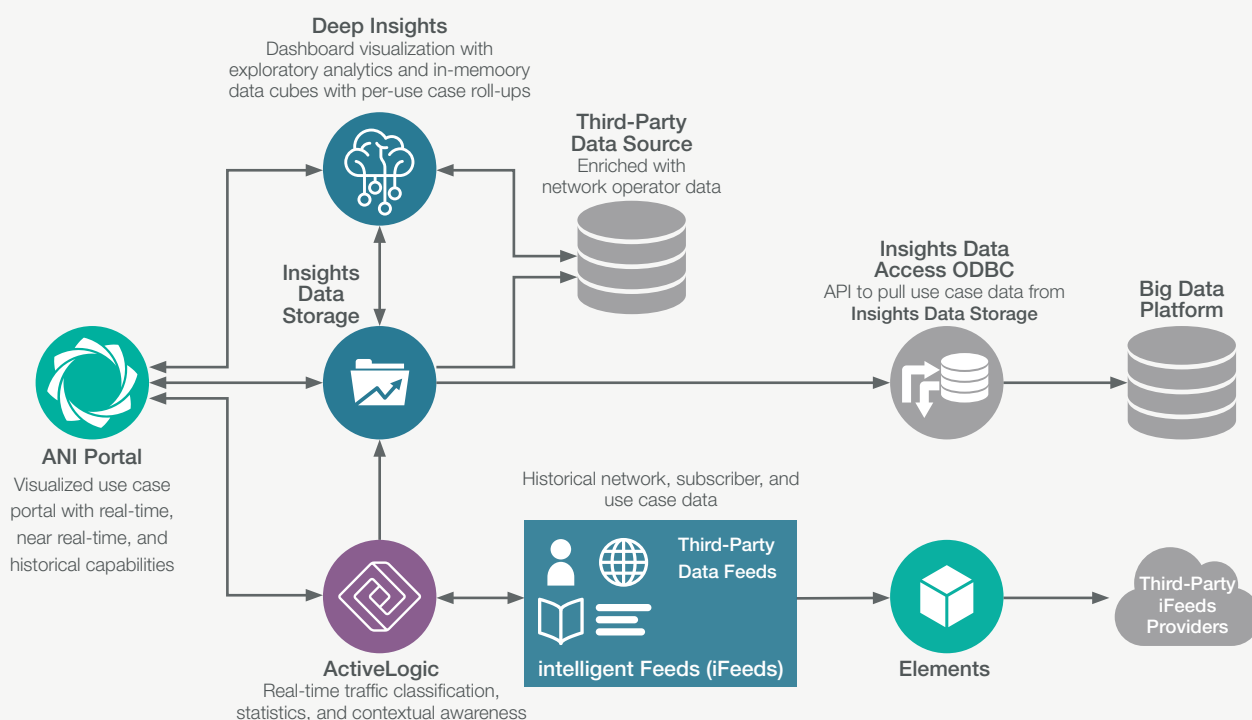
ContentLogic enables flexible content categorization of internet sites, enabling sophisticated policy enforcement or content-based charging.

The following ContentLogic databases are available from Sandvine:

- **Internet Watch Foundation (IWF):** Covers IWF feed of illegal child abuse images and websites, which is most suitable for regulatory requirements that mandate these sites to be blocked by all the operators.
- **Internet Filtering Database (IFD):** Covers URL categorization. This database is most suitable for use cases requiring generic URL categorization, such as Parental Control. It provides extensive and comprehensive web categorization and threat intelligence with domain, path, and page-level grouping. It gives four updates per day and offers a lighter version, IFD-Lite, which can be used for analytics and rulesets.

Figure 1

ANI Classification Engine with how the databases plug in



- **Internet Advertising Database (IAD):** Covers URL and ad categorization and is suitable for use cases requiring generic categorization, such as Parental Control. It also provides brand safety and contextual targeting, including subscriber analytics. Categories include: Content, Internet Advertising Bureau Tier1/2, IAB content rating, IAB non-standard and illegal content, Malicious, and whether URL is brand-safe and objectionable.
- **Cyber Threat Intelligence (CTI) Database:** Offers subscriber protection and empowers Sandvine's Cyber Threat Analysis and Cyber Threat Management use cases. The CTI database provides a real-time match against server hostname, IP addresses, ports, protocol ID, subnets, and URI, enabling detection of more than 40 types of cyber threats such as Botnet participation, botnet C&C communication, Cryptocurrency theft, phishing, and ransomware. Categorization and grouping of threats detected include malware name, malware family, malicious confidence, domain types, and MITRE/Kill Chain metadata for a detailed view on the attack lifecycle phases.

DeviceLogic

DeviceLogic provides in-depth details of a device used to generate HTTP and HTTPS traffic flows. The device properties or attributes are based on user-agents observed in the traffic flows. Some of the attributes in DeviceLogic are name, manufacturer, hardware type etc.

GeoLogic

GeoLogic enriches ANI data with categorized destination IP addresses mapped to geographic locations (country, region, and city), internet service provider registry details along with latitude/longitude details.

Microsoft Office 365 OTT

Microsoft Office 365 OTT enables granular classification of Microsoft Office 365 services. Rather than classifying traffic as simply Office 365, traffic for Exchange, SharePoint, MS Office Common, and Skype can be uniquely identified.

Table 1

Enhanced use cases

iFeeds	Use Cases	Delivers
ContentLogic	<ul style="list-style-type: none"> • Parental Control • Cyber Threat Analysis • Cyber Threat Management 	<ul style="list-style-type: none"> • Parental Control/Analytics /Demographics • Targeted Digital Advertisements • Customer Retention • URL Filtering • Application Control • Time-of-Day Control – e.g., No Social Networking During Homework Time • Detection of more than 40 types of cyber threats • Categorization and grouping of threats detected
GeoLogic	<ul style="list-style-type: none"> • Cyber Threat Analysis 	<ul style="list-style-type: none"> • Geo-Fencing – e.g., Block Country-Specific Content • Target Online Advertising • Localized Content • Enhanced Cybersecurity
DeviceLogic	<ul style="list-style-type: none"> • Subscriber Service Analysis 	<ul style="list-style-type: none"> • Device Specific Traffic Management • Analytics and Demographics • Venue-Based Advertising
Microsoft Office 365 OTT	<ul style="list-style-type: none"> • Performance Monitoring and Analysis 	<ul style="list-style-type: none"> • Classification of Office 365 Traffic <ul style="list-style-type: none"> • Application Control • Office 365 Subscription Management and Plan Status

iFEEDS MANAGEMENT

iFeeds offers a unique framework, which integrates purpose-built databases into Sandvine's industry-leading classification infrastructure, enabling the ANI Classification Engine to be extensible and flexible when more detailed context is needed on network traffic. It uses an automated, highly scalable file-based distribution infrastructure that is geographically redundant to ensure high availability for mission critical classification feeds (**Figure 2**).

Each ActiveLogic instance connects to the Sandvine iFeeds distribution network. To maximize deployment flexibility, the following topologies are supported:

Single ActiveLogic Node

- Databases are stored on the ActiveLogic server, which is connected to the Sandvine server

Multiple ActiveLogic Nodes

- Elements connected to the Sandvine server and ActiveLogic connected to the Elements as its source
- ActiveLogic downloads the database from Elements
- ActiveLogic has the choice to enable database as per the use case

In practice, one ActiveLogic can support ContentLogic, another ActiveLogic can support GeoLogic, etc.

Figure 2

iFeeds Data Flow

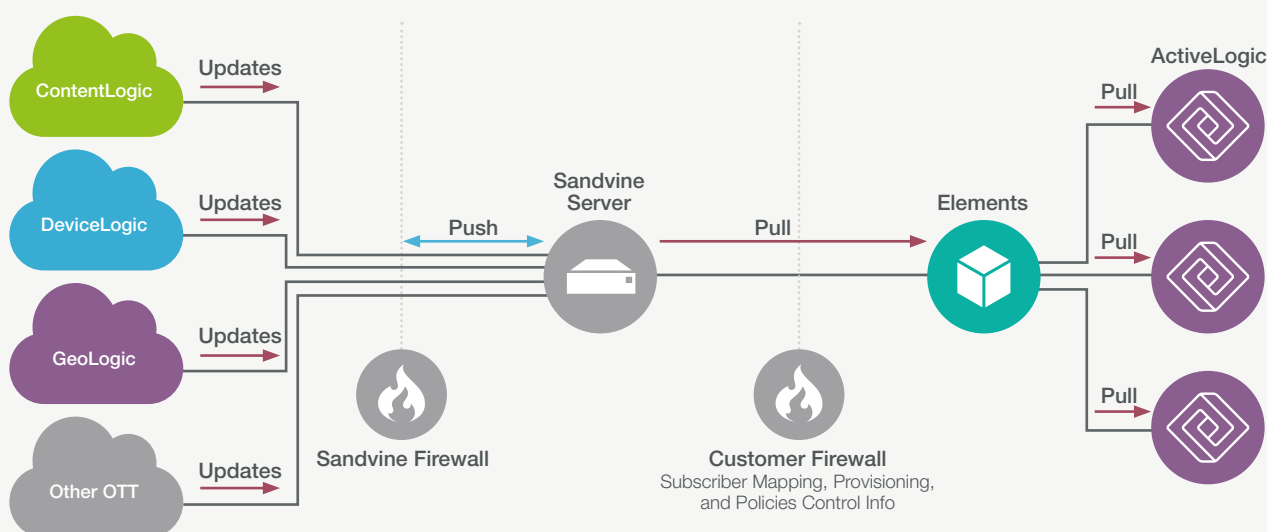
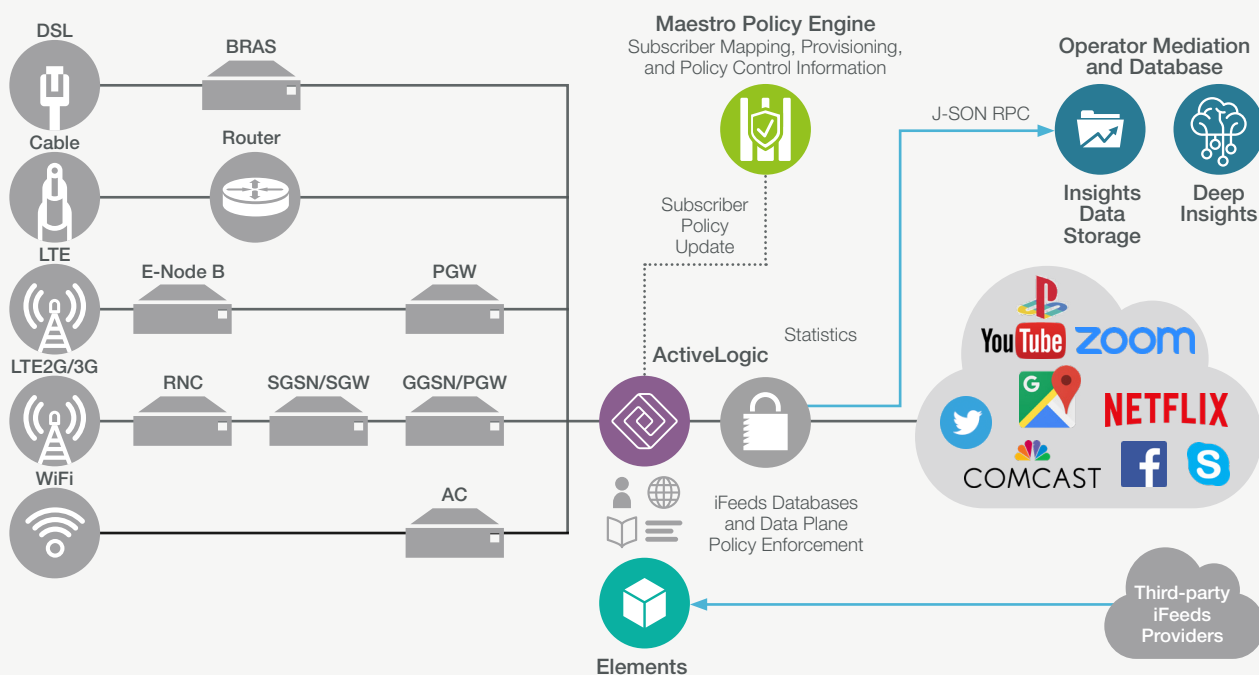


Figure 3 shows the deployment of Sandvine's iFeeds database for URL categorization, ContentLogic, in a customer network for the parental control use case. ContentLogic supports multiple content categories that are most suitable for Parental Control, including frequently updated phishing and malware categories to increase protection from security risks. Using a combination of policies, including content category, application, device and time-of-day, provisioned through standard API, converged operators can offer a compelling network-based parental control offering.

Figure 3

Typical iFeeds deployment in customer network



iFeeds equips operators with relevant, accurate, and useful data feeds to tackle the next era of network challenges. With iFeeds, operators have an ongoing stream of structured data with updates of current information from one or more sources in real time to drive additional context and enhance Sandvine's ANI use cases.

ABOUT SANDVINE

Sandvine's cloud-based Application and Network Intelligence portfolio helps customers deliver high quality, optimized experiences to consumers and enterprises. Customers use our solutions to analyze, optimize, and monetize application experiences using contextual machine learning-based insights and real-time actions. Market-leading classification of more than 95% of traffic across mobile and fixed networks by user, application, device, and location creates uniquely rich, real-time data that significantly enhances interactions between users and applications and drives revenues. For more information visit <http://www.sandvine.com> or follow Sandvine on Twitter @Sandvine.



USA
5800 Granite Parkway
Suite 170
Plano, TX 75024
USA

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

CANADA
410 Albert Street,
Suite 201, 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

Copyright ©2022 Sandvine Corporation. All rights reserved. Any unauthorized reproduction prohibited. All other trademarks are the property of their respective owners.

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.