QOSMOS

Product Datasheet

Protocol and Application Plugin & Signature Library

Qosmos ixEngine® is the most complete DPI engine on the market, with the ability to identify all major protocols and applications circulating on fixed and mobile networks. The technology goes beyond traditional DPI by extracting additional information in the form of metadata and by classifying encrypted traffic.

Key Facts

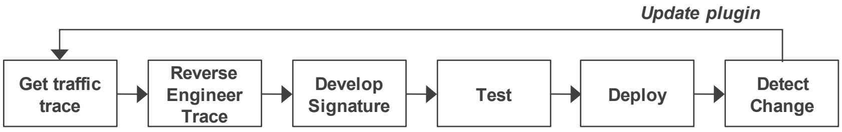
- Classification of application & protocol-IDs: 2,700 signatures available
- Extraction of metadata up to OSI Layer 7: 4,500 metadata available
- Supported by Qosmos Labs, a world-class team of protocol experts
- Nearly all network-based applications identified including mobile apps
- Identification of services (e.g. VoIP, chat, or file transfer) within applications
- Fast protocol plugin updates to maintain the ability to accurately classify IP flows
- Protocol plugins In-Service Software Upgrade (ISSU)
- On demand development of customized protocol plugins and signatures
- Custom Signature Module (CSM) to create customized signatures for any category of application including URLs, HTTP based applications, binary applications, etc.
- Almost all the signatures are in data format, securing the overall system integration

Qosmos ixEngine typically recognizes over 97% of network traffic including local and regional applications. Our library of more than 2,700 plugins and signatures covers all categories of protocols and applications used on IP networks by individuals (web and enterprise applications) and systems (Machine-to-Machine communications).

Qosmos Labs: A Team of Protocol Experts

Qosmos Labs has accumulated more than 10 years of expertise in identifying IP protocols and applications and detecting their changes. This is the company's most valuable asset which enables us to remain one step ahead of the competition and provide our customers with the most complete and reliable DPI and metadata extraction engine. Our international team of protocol experts and developers work around-the-clock gathering traffic samples, reverse engineering new protocols and designing new tools to make our engine more accurate. Our long experience ensures a solid software supply chain based on robust processes and in-house tools that we have developed to detect protocol changes and develop plugins quickly, while ensuring the highest standards of quality.

Qosmos Labs Software Update Process



Qosmos Labs software update process has been designed to ensure the identification and updates of a very large number of protocols and applications with minimum latency and maximum quality. This requires specific skills, organization, automation tools and procedures for developers and special features in the DPI engine to support fast updates.

Protocol and Application Identification

Each protocol or application decoder is called a "protocol plugin" or "signature". It contains the logic to classify an IP flow and to extract the associated metadata attributes and the content of those applications. A plugin identifies the layered networking protocols or applications inside the data stream, such as Ethernet.ip.tcp.http.facebook.facebook_mail. The Qosmos plugin library contains plugins for all categories of protocols and applications, from layer 2 protocols to layer 7 applications. The list of plugins is constantly evolving as new applications emerge. This document lists a small sample of plugins that we provide. For a complete and up-to-date list, please contact us.

Examples of Protocol and Application Identification

- Networking L2-L4: all protocols on IP networks
- Tunnels and VPN: GRE, L2TP, PPP, GTP, HTTP tunnel, Megaproxy, OpenVPN, etc. Classification of up to 16 levels of encapsulation
- Streaming media: YouTube, Netflix, Flash, PPLive, iTunes, ShoutCast, Spotify, Waze, etc.
- Social networking: Facebook including identification of applications within Facebook, Twitter, LinkedIn, Hi5, Sina, Weibo, Bebo, etc.
- Messaging and multi-conferencing: Skype, WhatsApp, Tango, Viber, Yahoo Messenger, 050Plus, Facetime, Line, KaKao Talk, Kaixin, WebEx, etc.
- VoIP: WeChat, iCall, Jabber, QQ, Telegram, Skinny, MCS, etc.
- Mobile apps: App Store, BlackBerry Messenger, iCloud, Shazam, Google Play, etc.
- Web browsing: full analysis of the HTTP protocol, top 50 websites for main regions (China, USA, Europe), hundreds of URLs, instant addition of URL-based plugins
- P2P: BitTorrent, eDonkey, Ares, Gnutella, Xunlei, iMesh, Kugou, etc.
- Games: Zynga games, Candy Crush, Angry Birds, Playstation Network, WiiConnect24, Xbox Live, 9game, etc.

Decoding of Advanced Network Behavior

Qosmos ixEngine not only decodes IP-based applications under normal traffic conditions, but also provides the best accuracy in the case of complex network configuration (e.g. HTTP proxy, HTTP pipelining, tunneling), when traffic is malformed, unidirectional or incomplete, and in the case of encryption and obfuscation. This capability is required to:

- Augment classification accuracy for use cases where completeness is key (application-based charging, QoE etc.)
- Foil DPI evasion techniques by inspecting tunnels that users may implement to hide unauthorized traffic
- Enable deeper classification by identifying applications inside tunnels

Encrypted / Obfuscated Traffic Analysis

There is an increasing trend towards more encrypted flows on IP networks, especially on mobile networks. By definition, a DPI engine is not able to read a packet payload which is encrypted. However, Qosmos ixEngine can identify the application behind most encrypted flows by using advanced techniques like statistical flow analysis, session prediction, peer matching and certificate inspection.

Qosmos can identify the following encrypted flows:

- HTTPS/SSL encrypted flows
- Encrypted P2P protocols like BitTorrent
- Applications that use their own encryption protocol like Skype. Qosmos can also identify services like VoIP and chat within Skype by using statistical recognition.
- IPSec tunnels
- Session prediction based on DNS cache

Delivery of Metadata

Qosmos ixEngine extracts 6 main categories of network-based application metadata and computed metadata**:**

- Volume: e.g. the volume of traffic per application and per user, size of a web page including all its components
- Application usage: e.g. Service type in Skype (audio/video, chat, file transfer, SkypeOut). Qosmos delivers more than 4,300 application metadata to enable smarter decisions based on full understanding of user behavior
- Application performance: e.g. delay and jitter / application / user, Qosmos also provides computed metadata like VoIP MOS and RFactor
- Identifiers: e.g. email sender / receiver addresses or any other ID that can be used to implement strong security rules
- Content: e.g. attached file within an email, which can be directed to specific processing like anti-virus or content inspection
- File metadata like codec and bit rate used in a Flash video. These metadata can be used for a wide array of applications such as customer experience management, network security, etc.

Example of metadata extracted for each HTTP request:
Full URI, User Agent, Error Code, Mime Type, Download size, Unitary Download time, is Download completed Y/N, Time to 1st response packet

Example of metadata extracted for each GTP tunnel:
Success/Failure Creation PDP Context, Time to establish PDP Context, IMSI/IMEI/IP Address, TEID, Location info, Cell ID, APN, GTP-C/GTP-U correlation

Example of metadata extracted for video streams (YouTube, Flash, RTP, etc.):
QoS Metrics (jitter, delay), Video information (e.g name), Bit rate, Instant Throughput (indicates whether a video has enough bandwidth to play with good quality), Codec, Re-Buffering Event, Download Completeness etc.

Always Up-To-Date

Applications and their protocols change constantly and without notice. Qosmos ixEngine provides the more secure path to reliable, always up-to-date DPI technology. Experts at Qosmos Labs continuously receive information about changes in protocols and applications and update the plugins.

Qosmos has developed specific productivity tools to speed up the protocol plugin development process while ensuring the highest standards of quality and reliability.

Creating Custom Signatures

The Custom Signature Module (CSM) gives ixEngine users the flexibility and independence to develop their own custom protocol signatures. This toolkit is particularly useful to develop signatures for local, proprietary or legacy protocols in a short period of time for securing customer roadmaps and SLAs. This is especially useful in enterprise environments, with internal domain names or in-house, proprietary protocols. End-users of products embedding ixEngine can also develop new signatures themselves.

In addition, Qosmos Labs can also develop any new protocol signatures upon request.

QOSMOS
The Network is Information

Qosmos is the leader in embedded Deep Packet Inspection and L7 Network Intelligence for use in physical, virtualized and SDN architectures. The company's software development kit and components are embedded by vendors and integrators into their products sold to telcos and enterprises. For more information: www.qosmos.com