Qosmos ixEngine

Market’s Leading DPI Engine, optimized for IA

November 2012
Did You Know?

On average, a Webmail protocol changes 3 times per year without warning or specs

The HTTP protocol uses 10x the CPU power than any other protocol

Next generation telecom and cyber security applications will not function without traffic metadata

80% of telecom vendors say it is becoming harder to keep up with rate of change in protocols

Fast time-to-market is the single most important business success factor in high-tech

3rd generation DPI will accelerate technology outsourcing

Reverse engineering protocols cannot use a classic product development process

70% of telecom vendors use DPI technology today and an additional 20% will during 2012

80% of telecom vendors say it is becoming harder to keep up with rate of change in protocols
Qosmos: Feeding Detailed Traffic Visibility to Applications

Visibility on 1,000+ application protocols

Extraction of 5,000+ Metadata
Caller, called party, jitter, packet loss, latency, call duration, setup time, codec, throughput, mobile ID (IMSI, IMEI), phone number, user login, IP address, MAC address, date & time of login / logoff, subject of email / chat / Webmail, sender, receiver, attached documents, response time, data transfer sessions (type, content, time), visited Website, page content, time spent on visit, basket share, referent, etc.

Embedded DPI & Network Intelligence
3rd Generation DPI/NI is Disruptive

Qosmos Offering in Line with Best-In-Class Strategy

Technology: 1st generation DPI
Strategy: internal development

Technology: 2nd generation
Strategy: outsourced dev. tools

Technology: 3rd generation
Strategy: outsourced dev. tools, application-specific products, services
3rd Generation DPI/NI is Disruptive

Qosmos Offering in Line with Best-In-Class Strategy
## DPI: Content Inspection or Network Analysis?

<table>
<thead>
<tr>
<th></th>
<th>Content inspection (Sensory)</th>
<th>L4-L7 Network Analysis (Qosmos)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method</strong></td>
<td>DPI: Inspect the Content of the packets/flows and not only the headers</td>
<td></td>
</tr>
</tbody>
</table>
| **Objective / features**| Detect 100k’s of virus/file signatures inside documents                                      | Recognize & analyze protocols and applications  
Fully decode a protocol to extract metadata                                                   |
| **How it works**        | Lexer: Detect patterns / regular expressions                                                 | Parser: Multiple algorithms used such as pattern matching, flow correlation, behavior analysis |
| **Implementation**      | Can be software (PCRE, Sensory Networks) or hardware (CaveCreek, …)                         | Software only (e.g. Qosmos ixEngine)                                                             |
| **Found in**            | IDS/IPS/AV                                                                                  | Next generation Firewall, NBAD, Forensics                                                        |
**Metadata are Becoming “Must Have”: Requires Advanced Expertise**

<table>
<thead>
<tr>
<th>Use case</th>
<th>Classification</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic traffic shaping</td>
<td>Must have</td>
<td>Not relevant</td>
</tr>
<tr>
<td>Traffic policy enforcement</td>
<td>Must have</td>
<td>Must have</td>
</tr>
<tr>
<td>QoS/CEM</td>
<td>Must have</td>
<td>Must have</td>
</tr>
<tr>
<td>Web analytics</td>
<td>Must have</td>
<td>Must have</td>
</tr>
<tr>
<td>Next Gen Firewall, IPS / IDS</td>
<td>Must have</td>
<td>Must have</td>
</tr>
<tr>
<td>Network forensics</td>
<td>Must have</td>
<td>Must have</td>
</tr>
</tbody>
</table>

**Extensive metadata extraction**

- **Yahoo! Mail**: Sender, receiver, login, subject, message +50 other
- **HTTP**: URL, Browser, cookies, DNS, authentication, +60 other
- **TCP**: Source port, destination port, client port, server port ...
- **GTP**: Device, user location, QoS metrics, time/duration ...
- **UDP**: Source port, destination port, client port, server port ...
- **IP**: Source/dest. address, source/dest. port, data ...

**DPI**

**Network Intelligence**

**QOSMOS**
Qosmos Core Technology
Embedded DPI & NI Traffic Decoding

Networking
- GTP, L2TP, ICMP, ...

Streaming
- YouTube
- Email
- Messaging
- Social NW

DPI / Network Intelligence Engine
- Flow classification + correlation
- Metadata extraction

Your Application Program
- Application ID
- Metadata
- Content

Packets
- Streams

C Library APIs

Qosmos Labs
- Protocol watch
- Productivity tools
- Procedures

Hot updates
- Updated plugins
- New plugins

Dynamic Updates

+ Tools to develop your own protocol signatures

- Feedback from live traffic
- Protocol changes
- Unknown protocols
**Protocol Signature Strategy**

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Code</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>C Language</td>
<td>PDL</td>
<td>SPID</td>
</tr>
</tbody>
</table>

**PDL**

(description "qosmos")
(family "Custom")
(classify
  (regexp http.server "www.qosmos.com")
(c-code | /* For the header */
  #include "uqosmos.h"
  ) ; End of C-Code

**Equivalent C-Code**

```c
/* Call back used to classify the QOSMOS protocol. */
static ctb_uint32 uqosmos_is_proto(upacket_t *pkt, const ctb_uint32 layer_index) {
    /* Get the session context */
    uapp_cnx_t *uapp_cnx = pkt->uapp_cnx;
    /* Get the server name */
    ctb_uint32 http_server_len = 0;
    const ctb_uint8 *http_server = GET_FROM_HTTP_LEN(Q_HTTP_SERVER, &http_server_len);
    /* Check if the HTTP header is done */
    if (http_server == NULL) {
        if (HTTP_HEADER_IS_FINISHED()) {
            return UC_MAYBE;
        } else {
            return UC_NO;
        }
    }
    /* Check the server name (http_server finished with '\0') */
    if (uregexp_match_len("www.qosmos.com", http_server, http_server_len - 1)) {
        return UC.YES;
    }
    return UC.NO;
}
static int uqosmos_on_first_packet(upacket_t *pkt, const ctb_uint32 layer_index) {
    printf("First\n");
    return UC_OK;
}
static int uqosmos_on_packet(upacket_t *pkt, const ctb_uint32 layer_index) {
    printf("Hello\n");
    return UC_OK;
}
/* The stored attributes. */
static const ustored_attr_t uqosmos_stored_attr[] = {
    {"http", Q_HTTP_SERVER}, /* XXX: This is array MUST be finished by {NULL} */
    {NULL},
};
/* The bottom layers for the QOSMOS protocol. */
static const ctb_char* uqosmos_bottom_layers[] = {"http", NULL};
/* The structure ulayer_t for the QOSMOS protocol. */
ulayer_t __uqosmos_layer = {
    unique_id: Q_PROTO_QOSMOS, /* < 128 */
    desc: "qosmos",
    name: "Qosmos WebSite",
    family: "Custom",
    bottom_layers: uqosmos_bottom_layers,
    on_packet: uqosmos_on_packet,
    on_first_packet: uqosmos_on_first_packet,
    is_proto: uqosmos_is_proto,
    stored_attr: uqosmos_stored_attr,
    version: 1,
};
```
## Overview of Qosmos Offering

<table>
<thead>
<tr>
<th>Core Network Intelligence Technology</th>
<th>ixEngine</th>
<th>DPI &amp; metadata software engine (C-libraries)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ixMachine</td>
<td>Configurable, flexible DPI &amp; metadata appliance</td>
</tr>
<tr>
<td>Application-Specific Products</td>
<td><strong>Telecom: Blades &amp; Appliances</strong></td>
<td>Optimized DPI &amp; metadata for QoS, Subscriber Analytics, Content Optimization</td>
</tr>
<tr>
<td></td>
<td><strong>Cybersecurity: DeepFlow Probes</strong></td>
<td>Optimized DPI &amp; metadata for SIEM/NBAD, Network Analytics, DDoS Mitigation</td>
</tr>
<tr>
<td>Services</td>
<td><strong>Professional services</strong></td>
<td>Software architecture advice, specification, integration, testing, maintenance</td>
</tr>
</tbody>
</table>
Qosmos DPI Engine in the Overall Architecture

Application

Packet processing
traffic dispatch, packet mgt, encapsulation, routing,
(Wind River INP / 6WIND)

Content

Content Inspection (Sensory Network Hyperscan)

Protocol Stack

Abstraction Layer (WIND RIVER / 6WIND)

Linux / Intel DPDK / WIND RIVER DPDK / 6WIND DPDK

Core 1  Core 2  Core 3  …  Core n
### IA – increasingly popular for DPI based applications

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large network IO</td>
<td>Yes <em>(thanks to DPDK)</em></td>
</tr>
<tr>
<td>DPI code needs large cache</td>
<td>Large cache</td>
</tr>
<tr>
<td>Typical DPI rate / core / GHz</td>
<td>&gt; 100K Packets Per Second</td>
</tr>
<tr>
<td>Multicore loadbalancing</td>
<td>Intel RSS</td>
</tr>
<tr>
<td>Price / performance</td>
<td>Cost-effective processors</td>
</tr>
<tr>
<td>Easy-to-find developer expertise</td>
<td>Pervasive expertise in IA</td>
</tr>
<tr>
<td>Ease of development</td>
<td>Easy dev environment <em>(Linux)</em></td>
</tr>
<tr>
<td>Ability to deliver on roadmap</td>
<td>Track record of delivering on roadmap</td>
</tr>
</tbody>
</table>

**DPI requirements are very different than switching/routing requirements**
Key Reasons For Vendors To Outsource

1. Difficult to find engineers with DPI and reverse engineering skills
2. R&D budget pressure
3. Difficult to continuously update protocols and applications
4. Competitive pressure
5. Time to market pressure

Source: Embedded DPI: An Industry Survey by Heavy Reading, Graham Finnie, Chief Analyst, September 2011
Qosmos Business Model

Qosmos is a pure-play vendor of DPI and Network Intelligence technology (no complete solutions)
Qosmos Works as a Strategic Partner

Products
- ixEngine SDK
- ixMachine probes
- DeepFlow probes

Services
- Architecture advice
- Integration support
- Deployment assist

Partnership
- Technical roadmaps
- Co-marketing
- Business planning
Qosmos Partnership Model

**Eval**
- Evaluation Support
- Quick start Tutorial
- Architecture advice

**Build**
- PoC Support
- NI Integration, Performance & Project Support
- Deployment Support
- Qosmos development of new protocols, HW porting & features
- Qosmos onsite engineer

**Run**
- Revenue ramp-up
- RT Maintenance

**Partner**
- CxO Calls
- Qosmos development of new protocols, HW porting & features
- Ecosystem partners
- Strategy workshop

COMPANY CONFIDENTIAL
Qosmos International Presence

Americas
- San Francisco
- New York
- Washington

EMEA
- London
- Paris

APAC
- Singapore

Worldwide presence and support
Qosmos Ecosystem and Network Intelligence Alliance

Extended members of the Qosmos ecosystem

Solutions & SW Based on Network Intelligence

- Policy and Charging Control (PCC)
- Subscriber Analytics
- QoS / Quality of Experience
- Web Market Research
- Financial transaction tracking
- Cyber security
- Data analysis & visualization
- Etc.

Traffic Processing & Decoding Technology

- Extraction of metadata & content
- Traffic decoding
- Processing systems & platforms
- Packet capture and processing
Checklist When Choosing a DPI/NI Technology Partner

☐ Is the company well-established, with a stable customer base and investors?

☐ Is the business model aligned for strategic partnership?

☐ Does the company provide 3rd generation technology, able to handle high throughputs and decoding of large amounts of metadata?

☐ Does the decoding engine support all leading processor architectures (Intel, NetLogic, Broadcom, Cavium, Tilera, etc.)?

☐ Is the company able to provide development assistance and worldwide technical support?
Network Intelligence Technology: Where Do You See Yourself On This Matrix?

- Must have
- Nice to have

- Will develop internally
- Will outsource

[Diagram showing a matrix with questions]
Key Decision Factors for Make vs. Buy

- **Do you need detailed visibility of all network-based activity?**
  - Beyond traffic classification → also traffic metadata?
  - Do you require absolutely accurate information?
  - At multi-Gbps speeds?

- **Do you prefer to source DPI and network intelligence externally?**
  - Want to focus internal developers on building complete solutions?
  - Looking for pre-developed building-blocks?
  - Need to shorten product development times and accelerate time-to-market?
  - Want somebody else to keep up with constantly evolving Web applications and protocols?

*If you answered “YES” to these questions, Qosmos is the right partner for you!*