TEST REPORT

Tolly.

#222116

March 2022

Commissioned by

Cubro Network Visibility

Cubro Custos

Network Monitoring Functionality & Efficiency

EXECUTIVE SUMMARY

When it comes to network monitoring, network size doesn't matter. Local or global, small or large, it is essential for every company to have insights into network activity. Effective monitoring can provide critical insights into application usage, identify bottlenecks, and help reveal possible security threats. Cubro Custos is designed to be an intuitive and small-footprint network monitoring solution that provides critical insights into user and application activity.

Cubro Network Visibility commissioned Tolly to evaluate the usability, storage efficiency and approach to data structure used in Custos. Tests were run by evaluating a live network simultaneously using Cubro Custos and legacy NetFlow/IP Flow Information Export (IPFIX) files.

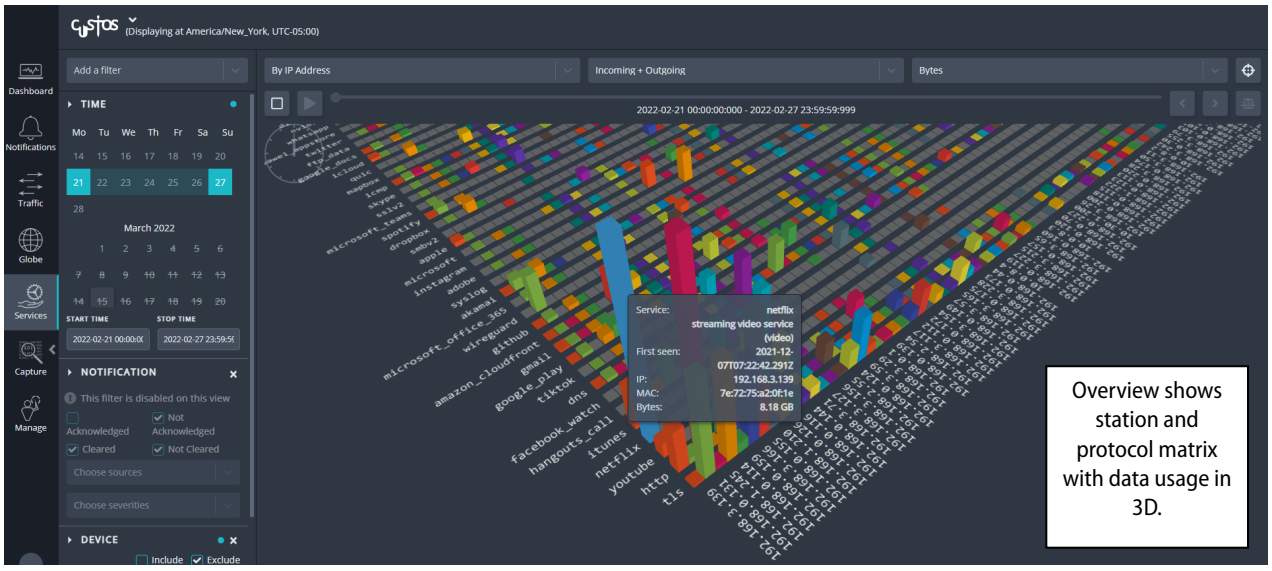
Tests showed that the Custos 3D-style user interface provided insightful, immediately actionable network information, stored network data dramatically more efficiently than NetFlow/IPFIX, and implemented a human-oriented data structure that could be easily integrated into 3rd-party systems.

THE BOTTOM LINE

Cubro Custos delivers:

1. Powerful and intuitive network monitoring
2. Time-Window Aggregation (TWA) that dramatically reduces file size for network transfer and storage; 35x smaller than NetFlow using default one minute window
3. Highly optimizable using custom collection window; 61x smaller than NetFlow using five minute time window
4. Data structure designed with human-readability in mind

Cubro Custos Network Monitoring Services Overview



Note: Filters can be applied to display screens in real time to allow network admins to highlight the most relevant information.

Source: Tolly, March 2022

Figure 1

Cubro Network Visibility

Custos Network Monitoring

Features & Efficiency

Tolly. Certified

Tested March 2022

Test Results

Cubro GUI

Ultimately, a network monitoring system is only as good as its user interface. It is the graphical user interface (GUI) that is needed to make sense out of the thousands of network events that are captured by the system and stored.

The Cubro GUI really speaks for itself. The use of color coding and three-dimensional mapping to illustrate application traffic levels of individual stations allows network administrators to pick out stations and applications quickly and easily for further analysis. This report will highlight several key views of the Custos GUI. To fully understand the power of the GUI, Tolly recommends that the reader view an online demonstration.

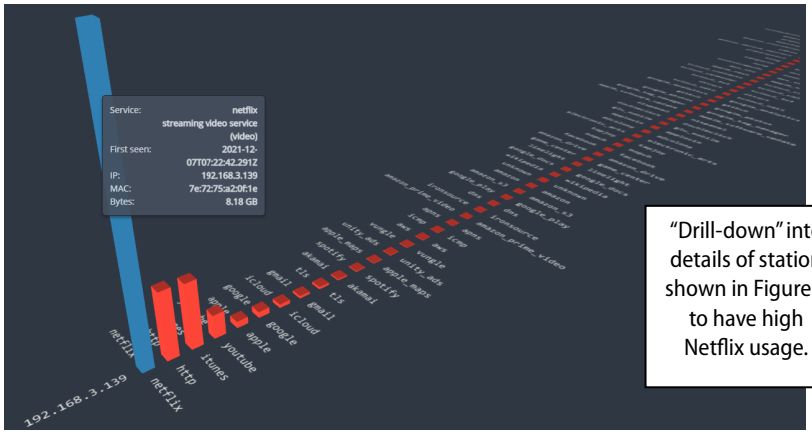
Service View

Shown in Figure 1 (previous page), the service view provides a visualization of hundreds (or more) of data points in a multi-dimensional matrix that cross references device IP addresses, applications/protocols and traffic statistics at a glance. The user can apply filters to the displayed data in order to focus on or isolate particular devices or applications. Hovering over a bar provides additional information such as time stamp, MAC address and exact byte counts. Figure 2 shows a detail view for a single device.

Devices Overview

This view organizes monitoring data with a device focus. The data can be quickly searched by IP address, MAC information, informational tags, etc. This view also provides "first seen" and "last seen" timestamps which can be very helpful

Cubro Custos Network Monitoring Services Overview

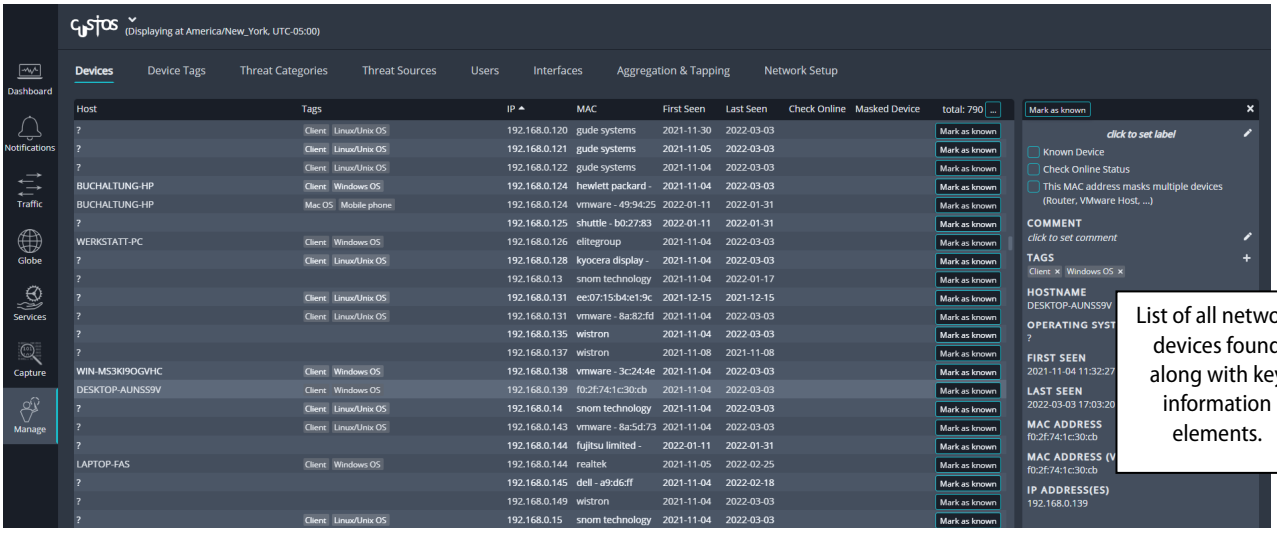


"Drill-down" into details of station shown in Figure 1 to have high Netflix usage.

Source: Tolly, March 2022

Figure 2

Cubro Custos Network Monitoring Devices Overview



List of all network devices found along with key information elements.

Source: Tolly, March 2022

Figure 3

when troubleshooting network problems. See Figure 3.

Traffic Source Overview

This view distills all network traffic into three categories: incoming, outgoing, and internal. When mapped with time-of-day and day-of-week, this can help rapidly identify anomalous traffic patterns. For example, outgoing traffic during an overnight period could identify data being surreptitiously exfiltrated from your network.

More generally, this can identify peaks that could represent WAN bottlenecks. See Figure 4.

Cubro Custos Network Monitoring Traffic/Source Overview

Source: Tolly, March 2022 Figure 4

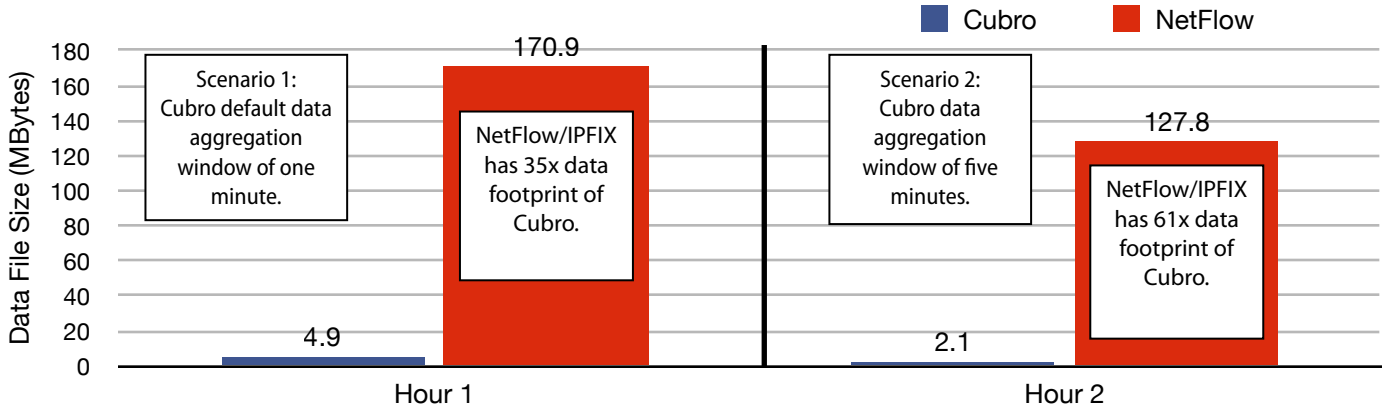
Storage Efficiency

Before network monitoring data can be analyzed and displayed, it must be collected and stored. Cubro's time-window aggregation method packages and stores data within a development-language-neutral container utilizing Google's Protocol Buffers (protobuf) format. This allows drastic data reduction at the point of collection. Contrast this to legacy NetFlow and IPFIX approaches where data reduction takes place at the analysis stage. Cubro's approach dramatically reduces both short-term and long-term storage requirements.

For this set of tests, data from a live network was collected simultaneously using Cubro's time-window aggregation (stored in protobuf format) and NetFlow. (See Figure 8.) Tests were run during two different hours of the day.

Storage Efficiency: Cubro Time-Window Aggregation vs. NetFlow

(Lower result is better)



Note: Separate tests monitoring live traffic during two different hours, thus differing file sizes for base NetFlow traffic. Cubro data stored in Google Protocol Buffers (protobuf) format.

Source: Tolly, March 2022 Figure 5

With Cubro's default aggregation window of one minute, the data file was 4.9 Mbytes where the NetFlow file was 35x as large.

When Cubro was set to a five minute time window and the test run again, the data file was 2.1 Mbytes where NetFlow was 61x as large. See Figure 5.

Data Structure

When Cubro developed its optimized time-window aggregation format, designers focused on making the data structure readily understood not just by machines, but by humans.

Cubro data field names such as "incoming Pkts" and "outgoing Bytes" are immediately understood by the people working with the data. Figure 6 shows the partial data structure and a quick glance reveals the easily-understood names in use throughout.

Figure 8 contains both an example analysis graphic along with the structured data that partially produced that graphic. This illustrates how Custos maps its data collection approach to how the data will be represented in the analysis GUI.

Cubro Custos Time-Window Aggregation Format

Custos data is structured to be understandable by humans.

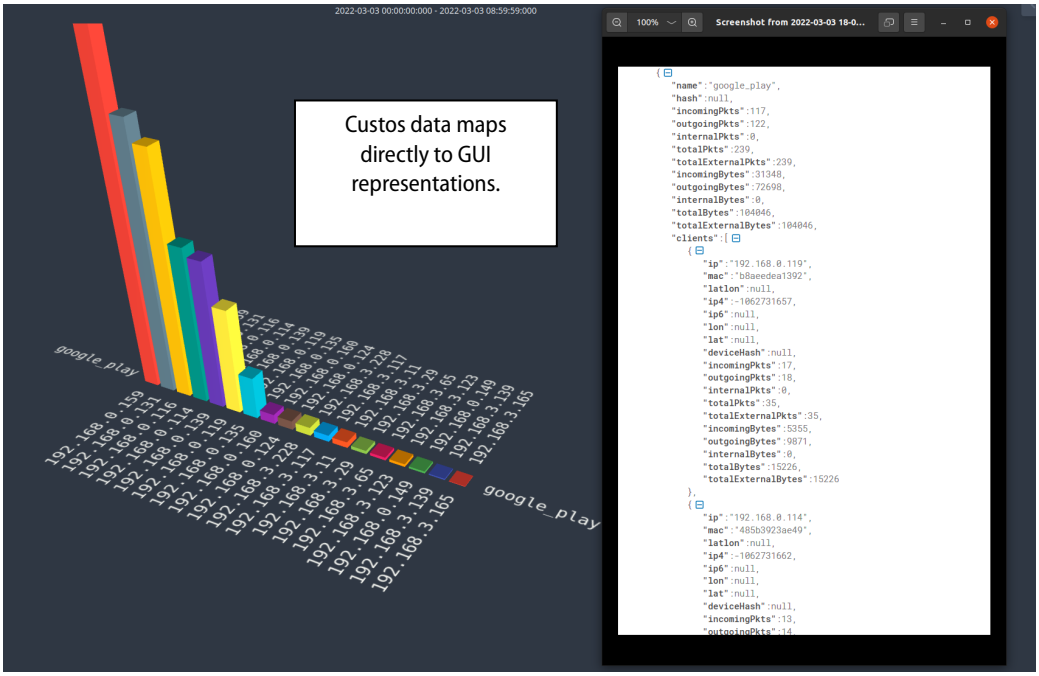
```
message TimeWindow {
  int64 timestamp = 1;
  int64 bps = 2;
  int64 incomingPkts = 3;
  int64 outgoingPkts = 4;
  int64 internalPkts = 5;
  int64 incomingBytes = 6;
  int64 outgoingBytes = 7;
  int64 internalBytes = 8;
  int32 connections = 9;
  repeated ServiceData services = 10;
  repeated ClientData clients = 11;
  repeated IpData servers = 12;
  repeated TypeBytesData l3 = 13;
  repeated TypeBytesData l4 = 14;
  repeated PortData ports = 15;
  repeated DnsData domains = 16;
}

message ServiceData {
  ServiceEntry service = 1;
  int64 incomingPkts = 2;
  int64 outgoingPkts = 3;
  int64 internalPkts = 4;
  int64 incomingBytes = 5;
  int64 outgoingBytes = 6;
  int64 internalBytes = 7;
  repeated IpData clients = 8;
  repeated IpData servers = 9;
}
```

Note: Partial representation of dataset.

Source: Tolly, March 2022

Figure 6

Cubro Custos - Example Mapping Data to Graphics



Source: Tolly, March 2022

Figure 7

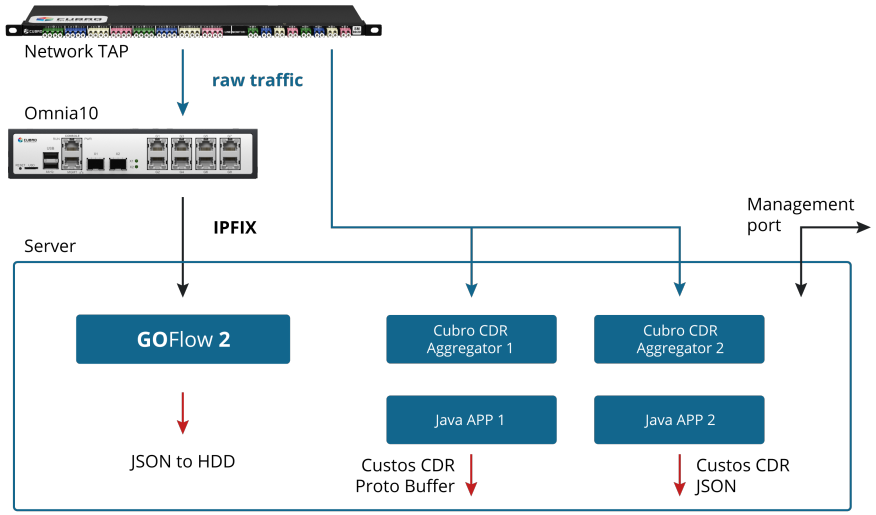
Third-Party Compatibility

Some users may want to integrate Cubro monitoring data into a third-party system or into some other analysis tool.

Tolly engineers verified that Cubro could also generate monitoring data in industry-standard JSON (JavaScript Object Notation) format (not shown) as an alternative to Protocol Buffers format.

While this method is not as data efficient as the Cubro time-window aggregation approach it is an important option for some customers.

Cubro Custos - Network Visibility Test Network & Data Collection Diagram



Note: Traffic was captured and forwarded to both Cubro aggregators and IPFIX (GoFlow2) collectors. To illustrate Cubro flexibility, the Custos output was saved in two formats: Google Protocol Buffers and open standard JSON.

Source: Tolly, March 2022

Figure 8

About Cubro Network Visibility & Custos

Cubro network visibility solutions remove network monitoring 'blind spots' to provide enhanced visibility and control of all data transiting a company's network.

Cubro's solutions are instrumental in the successful outcomes of IT initiatives such as 5G/4G/3G, customer experience management and service assurance, digital transformation, data security, virtualized data centers and software-defined networking/NFV.

Cubro launched its monitoring software Custos in 2021. Custos builds a comprehensive understanding of your network's behavior over time and provides a powerful advantage by identifying actionable items and potential issues before they become costly problems.

View the demo "Introduction to Custos: Network Guardian" at:
https://youtu.be/8ZqrC14NGEg

Source: Cubro Network Visibility, March 2022

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 30 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at
+1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

di-1-wt-2022-03-28-VerJ