

# Custos - Network Guardian Solution

November 2023

- Challenges of IT Infrastructure Management
- Custos - Introduction
- Features Overview
- Use Cases
- Customer Inquiries

# Challenges of IT Infrastructure Management

Networks are essential for conducting business and commerce in the modern world. Companies rely on networks for communication with customers, suppliers, and partners. E-commerce platforms leverage networks to enable online shopping and transactions.



Poor connectivity and lack of reliable network

Limited resources and dedicated IT personnel in small medium-sized enterprises



Misconfigured network devices

Reactive network monitoring strategy, which can result in downtime



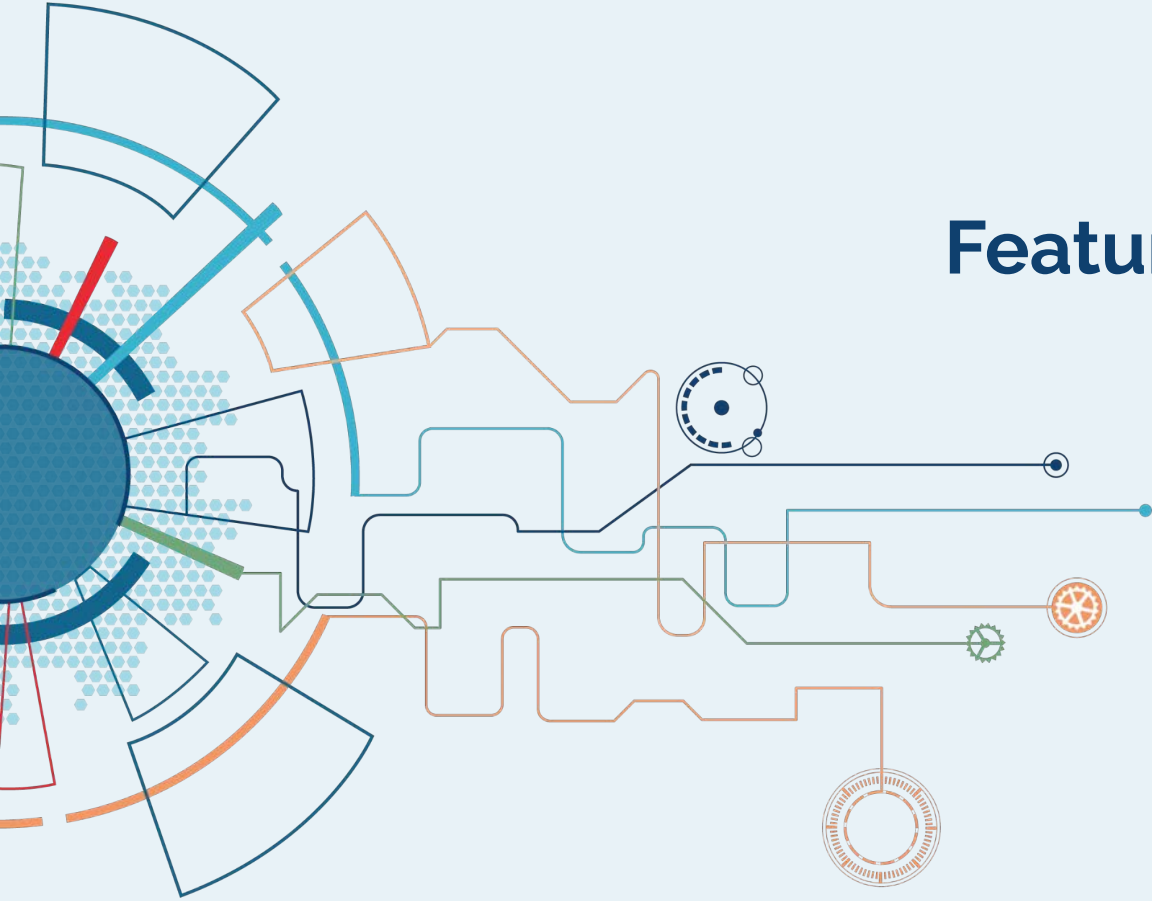
Time spent to detecting security threats and network outages

- An easy-to-use solution that protects small and midsize networks from external and internal threats.
- IT infrastructure and internet connectivity are crucial for all businesses, irrespective of the size.
- Main challenges for IT infrastructure owner / operator include:
  - ◆ External threats
  - ◆ Internal threats
  - ◆ Hardware and Software damage
  - ◆ Service Provider issues

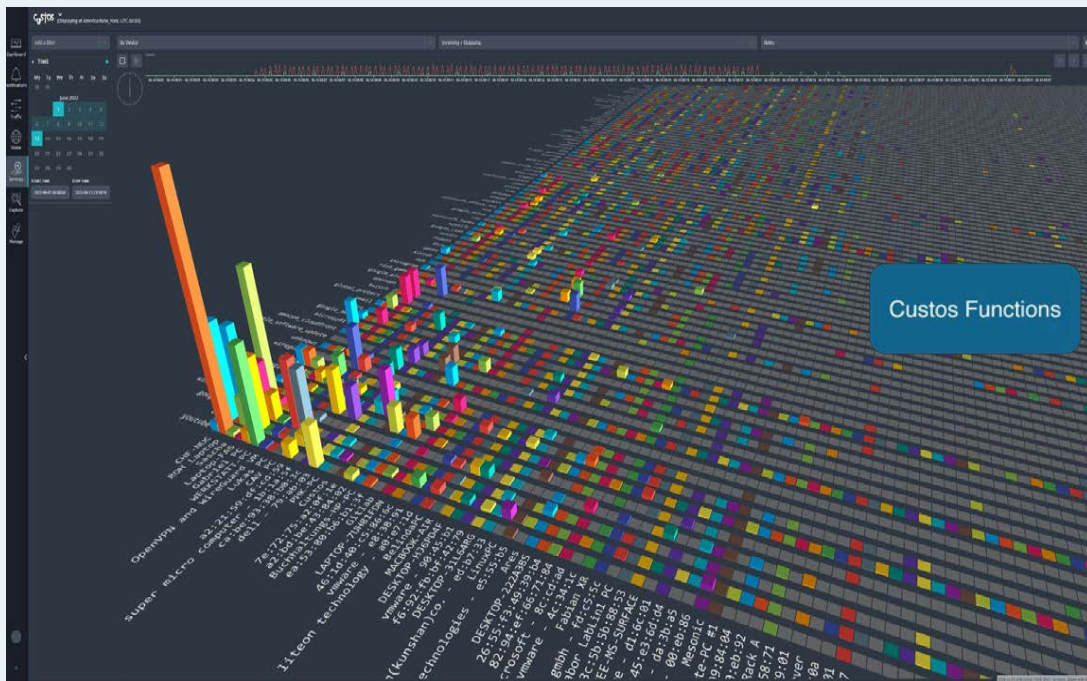


Custos

# Features Overview



# Features Overview



## General service statistics

Filtering DPI graphs

Up to 4000 services

Look for unwanted traffic

## Notifications

Threat Detection

New device on the network

Missing device on the network

## Traffic Bandwidth Statistics

Traffic per Subscriber/Client

Traffic per Application/Service

Bandwidth distribution over time

## Activate Network Scanning

Inventory Scan

Keep-Alive-Ping to prove device availability

## Export Data

Export stream via Kafka

Export to Excel/CSV on the fly

## Geolocation data

Performance statistics based on geolocation endpoints



# Small network connection diagram

For smaller deployments, Omnia120 is used to collect raw packets from various feeds within the networks.

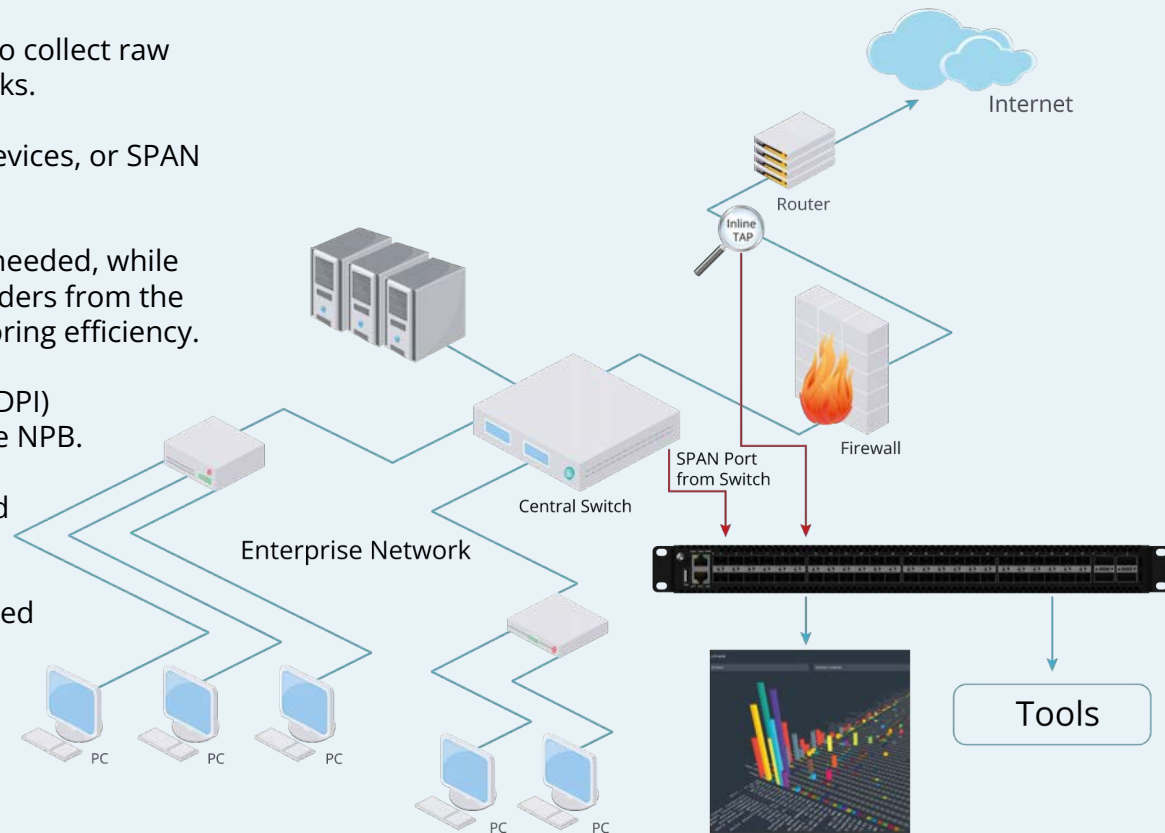
These feeds, originating from TAPs, Bypass devices, or SPAN ports, all linked to the Cubro Omnia120.

The NPB handles aggregation and filtering if needed, while also eliminating tunneling and unwanted headers from the packet, which subsequently enhances monitoring efficiency.

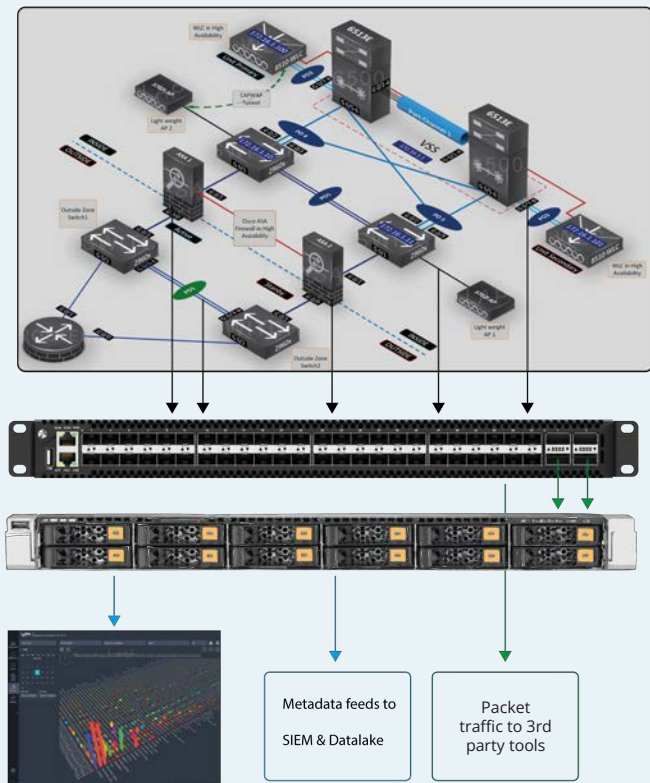
The raw traffic is then processed in the NPB (DPI) and presented through Custos running on the NPB.

Furthermore, the Cubro NPB can also forward copies of the raw traffic to 3rd party tools.

And finally, the Custos data can also be directed southbound to SIEM and Data lake solution for further processing.



# Large network connection diagram



For large deployments, Omnia120 or other network packet brokers are used to collect raw packets from different feeds in the networks.

These feeds, originating from TAPs, Bypass devices, or SPAN ports, are all linked to the Cubro NPB and the packet broker.

The NPB performs aggregation and filtering if needed and also removes tunnel and unwanted headers from the packet, which subsequently enhances monitoring efficiency.

Then the NPB load balances the raw packet traffic to Omnic Cards mounted in a server for analytics.

Furthermore, the Cubro NPB can also forward copies of the raw traffic to 3rd party tools.

The Omnic cards in the server do the DPI analytics, and the data is then stored on the server and presented via the Custos application running on the server.

And finally, the Custos data can also be directed southbound to SIEM and Data lake solution for further processing.



# Network Bandwidth

custos

Displaying at Europe/Vienna, UTC +01:00  
2023-11-21 12:11:15

Add a filter

Bits / Second

Select a few days and then zoom in to see details

TIME

Mo	Tu	We	Th	Fr	Sa	Su
30	31					
November 2023						
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

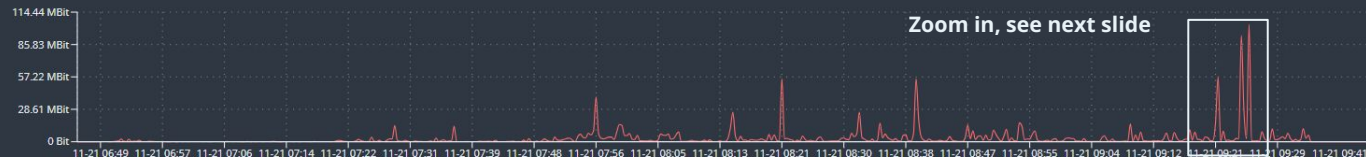
START TIME

2023-11-21 06:46:04

STOP TIME

2023-11-21 09:41:45

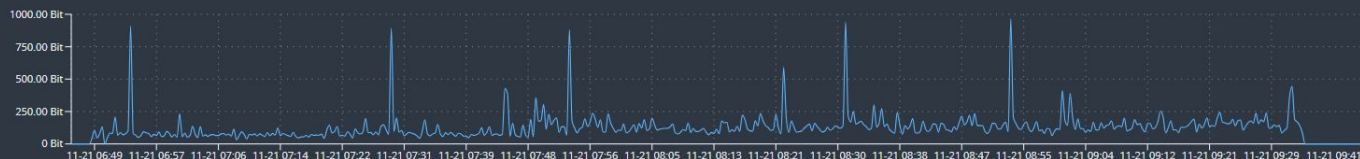
## Bits/Second (incoming)



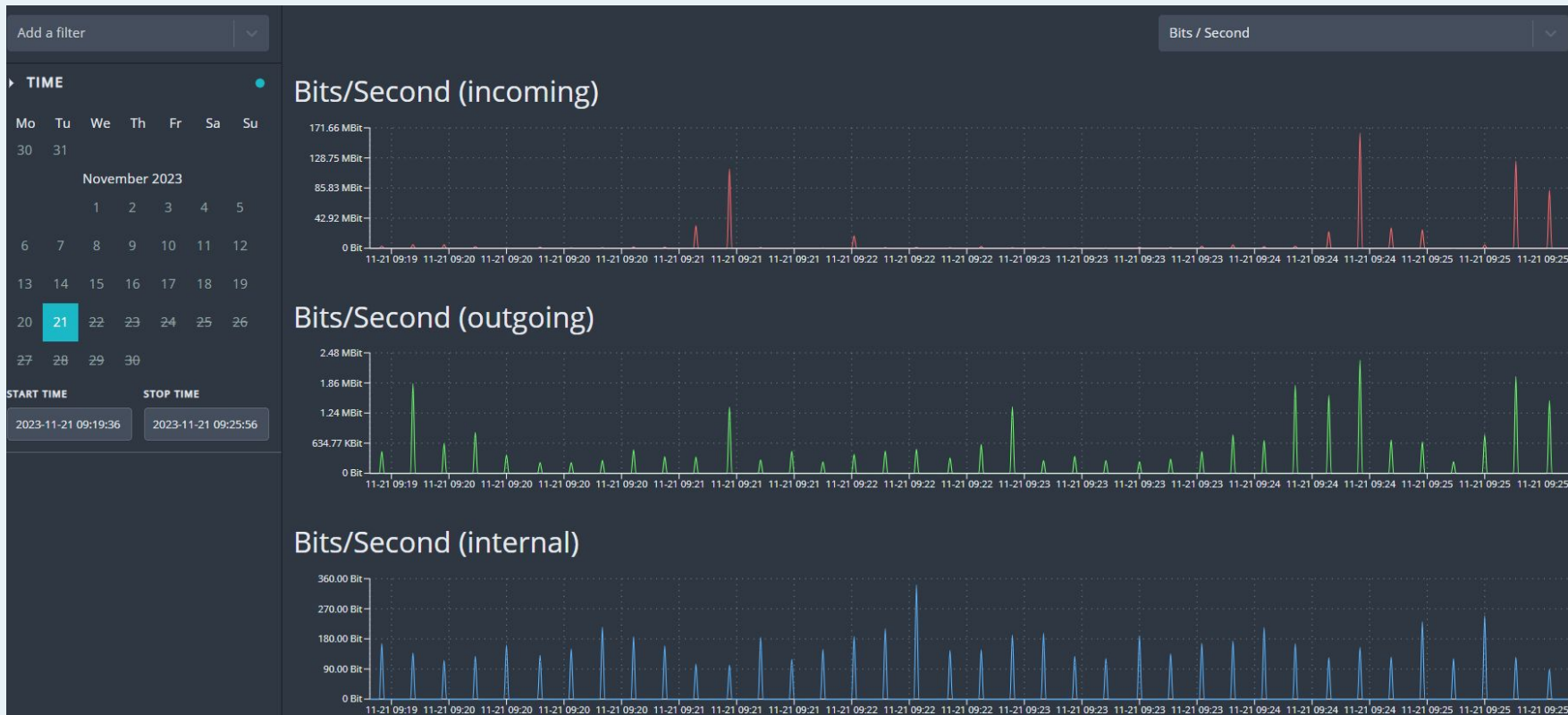
## Bits/Second (outgoing)



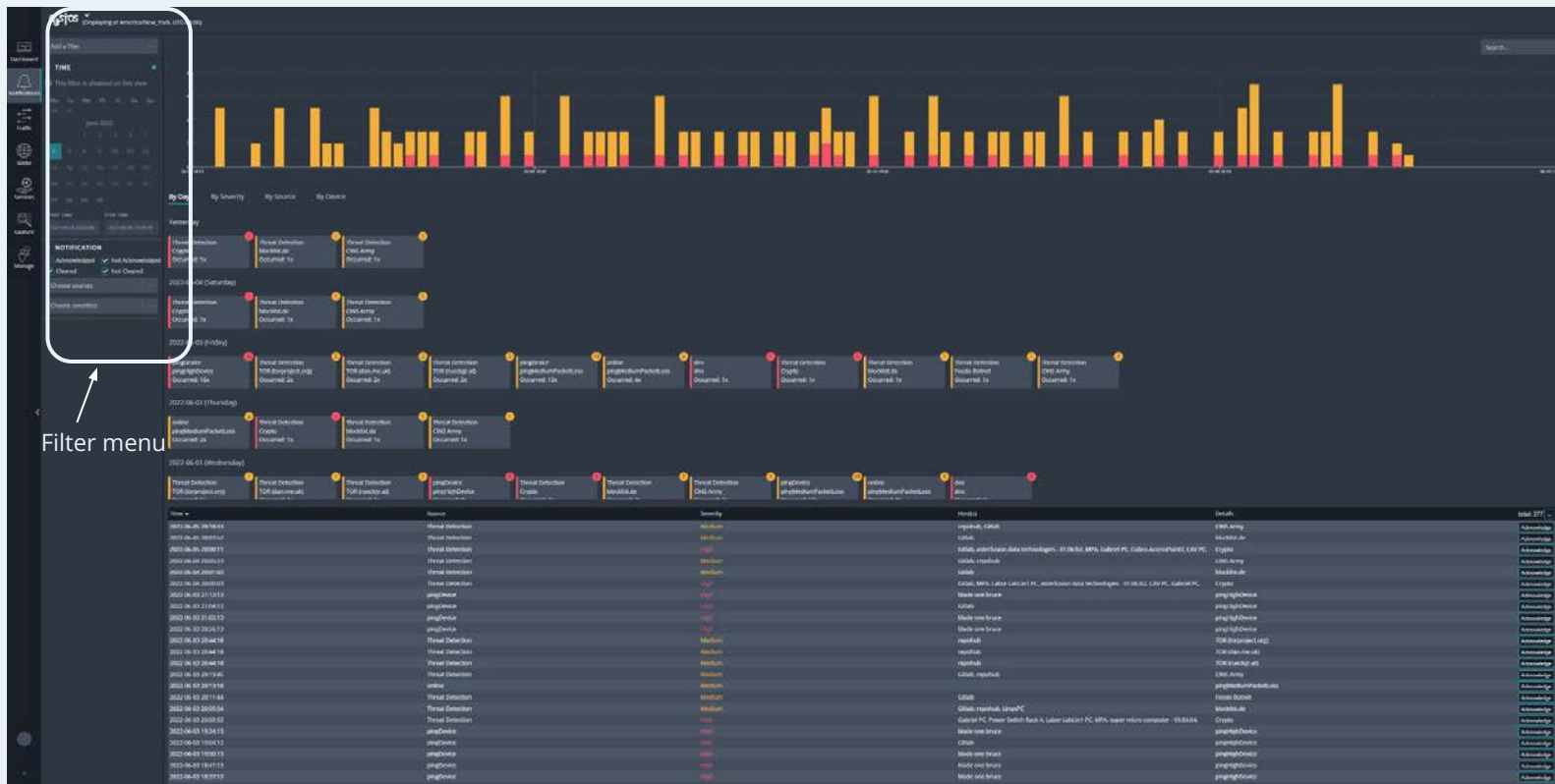
## Bits/Second (internal)



# Zoomed-in View



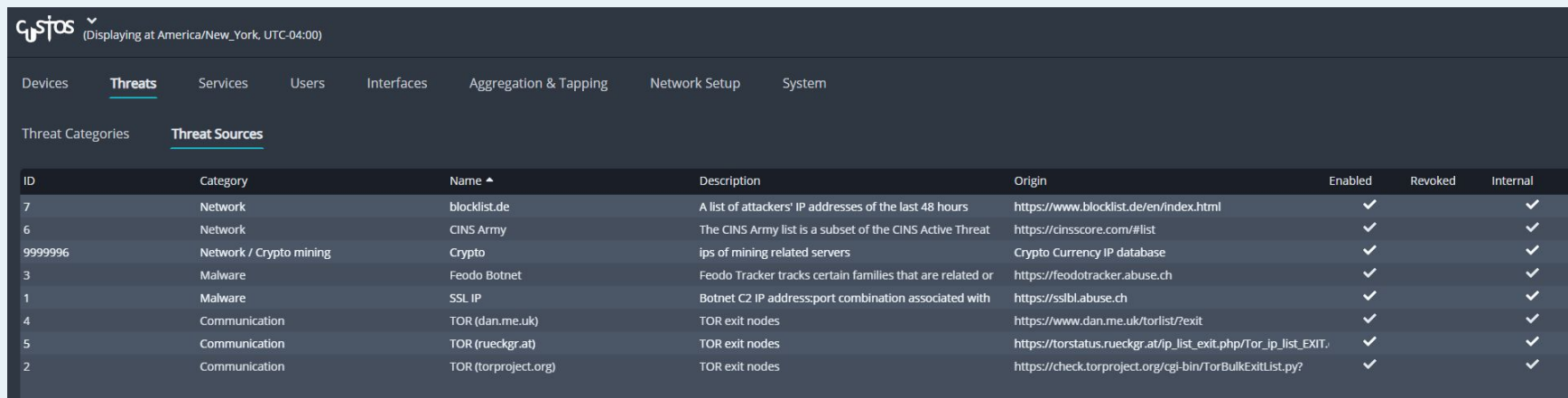
# Threat Notification screen



# How does threat detection work?

Constantly evolving threats from external devices pose challenges for SysOps and SecOps. Therefore, they invent common available IP lists that hold information about suspicious network device. These lists are continually updated.

Custos uses this lists to produce the Threat information. The sources for this are now visible in the UI → Manage—Threats—Threat Sources.



The screenshot shows the Custos web interface. At the top, it says 'Custos (Displaying at America/New\_York, UTC-04:00)'. Below this is a navigation bar with tabs: Devices, Threats (selected), Services, Users, Interfaces, Aggregation & Tapping, Network Setup, and System. Under the 'Threats' tab, there are sub-tabs: Threat Categories and Threat Sources (selected). The main content area displays a table of threat sources.

ID	Category	Name ^	Description	Origin	Enabled	Revoked	Internal
7	Network	blocklist.de	A list of attackers' IP addresses of the last 48 hours	<a href="https://www.blocklist.de/en/index.html">https://www.blocklist.de/en/index.html</a>	✓		✓
6	Network	CINS Army	The CINS Army list is a subset of the CINS Active Threat	<a href="https://cinsscore.com/#list">https://cinsscore.com/#list</a>	✓		✓
9999996	Network / Crypto mining	Crypto	ips of mining related servers	Crypto Currency IP database	✓		✓
3	Malware	Feodo Botnet	Feodo Tracker tracks certain families that are related or	<a href="https://feodotracker.abuse.ch">https://feodotracker.abuse.ch</a>	✓		✓
1	Malware	SSL IP	Botnet C2 IP address:port combination associated with	<a href="https://ssllbl.abuse.ch">https://ssllbl.abuse.ch</a>	✓		✓
4	Communication	TOR (dan.me.uk)	TOR exit nodes	<a href="https://www.dan.me.uk/torlist?exit">https://www.dan.me.uk/torlist?exit</a>	✓		✓
5	Communication	TOR (rueckgr.at)	TOR exit nodes	<a href="https://torstatus.rueckgr.at/ip_list_exit.php/Tor_ip_list_EXIT">https://torstatus.rueckgr.at/ip_list_exit.php/Tor_ip_list_EXIT</a>	✓		✓
2	Communication	TOR (torproject.org)	TOR exit nodes	<a href="https://check.torproject.org/cgi-bin/TorBulkExitList.py?">https://check.torproject.org/cgi-bin/TorBulkExitList.py?</a>	✓		✓

The respective source is automatically updated. The preconfigured sources have already set the default values so that it roughly matches the update interval of the list itself.

# Device Overview





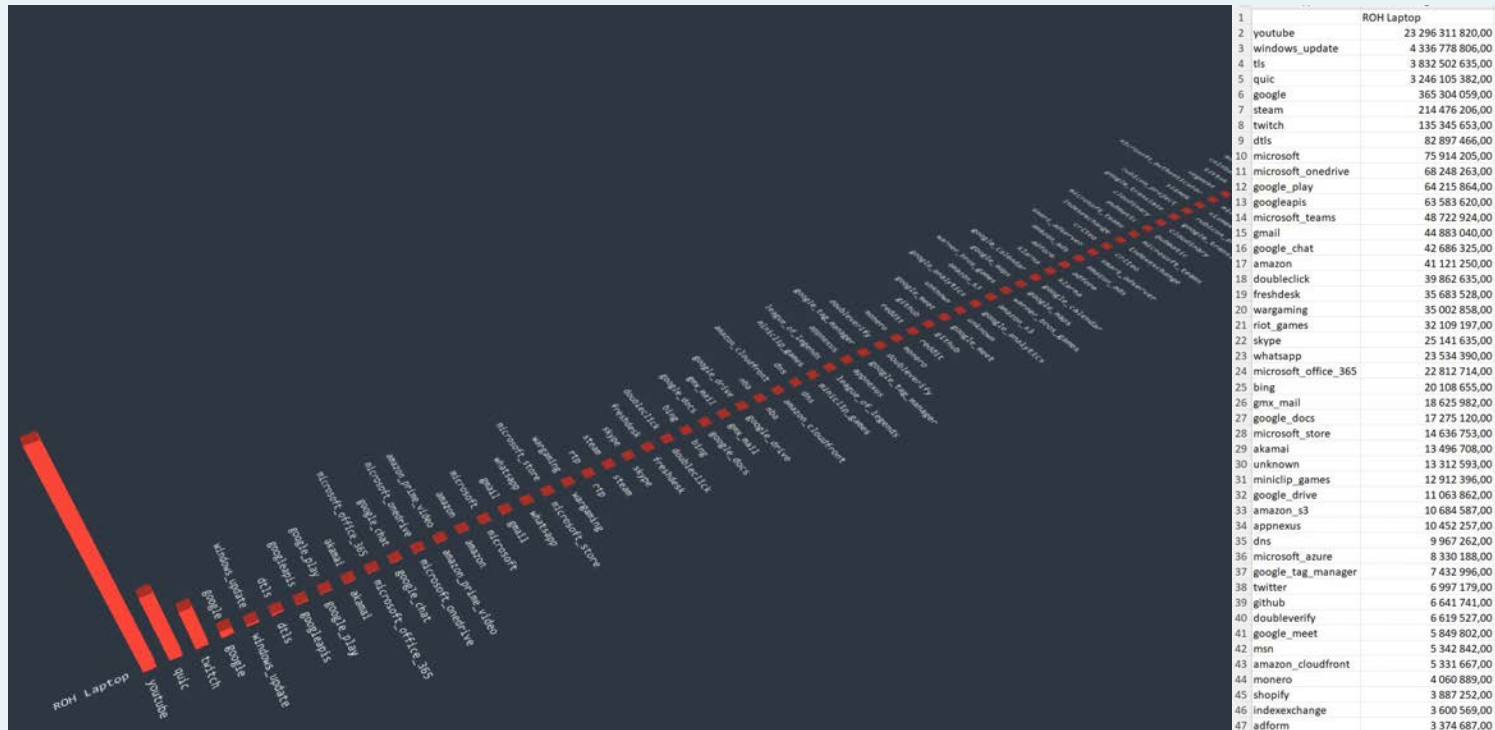
# Volume calculation of each individual subscriber in any different time frame Day/Week/Month/year can be exported to Excel

Excel export

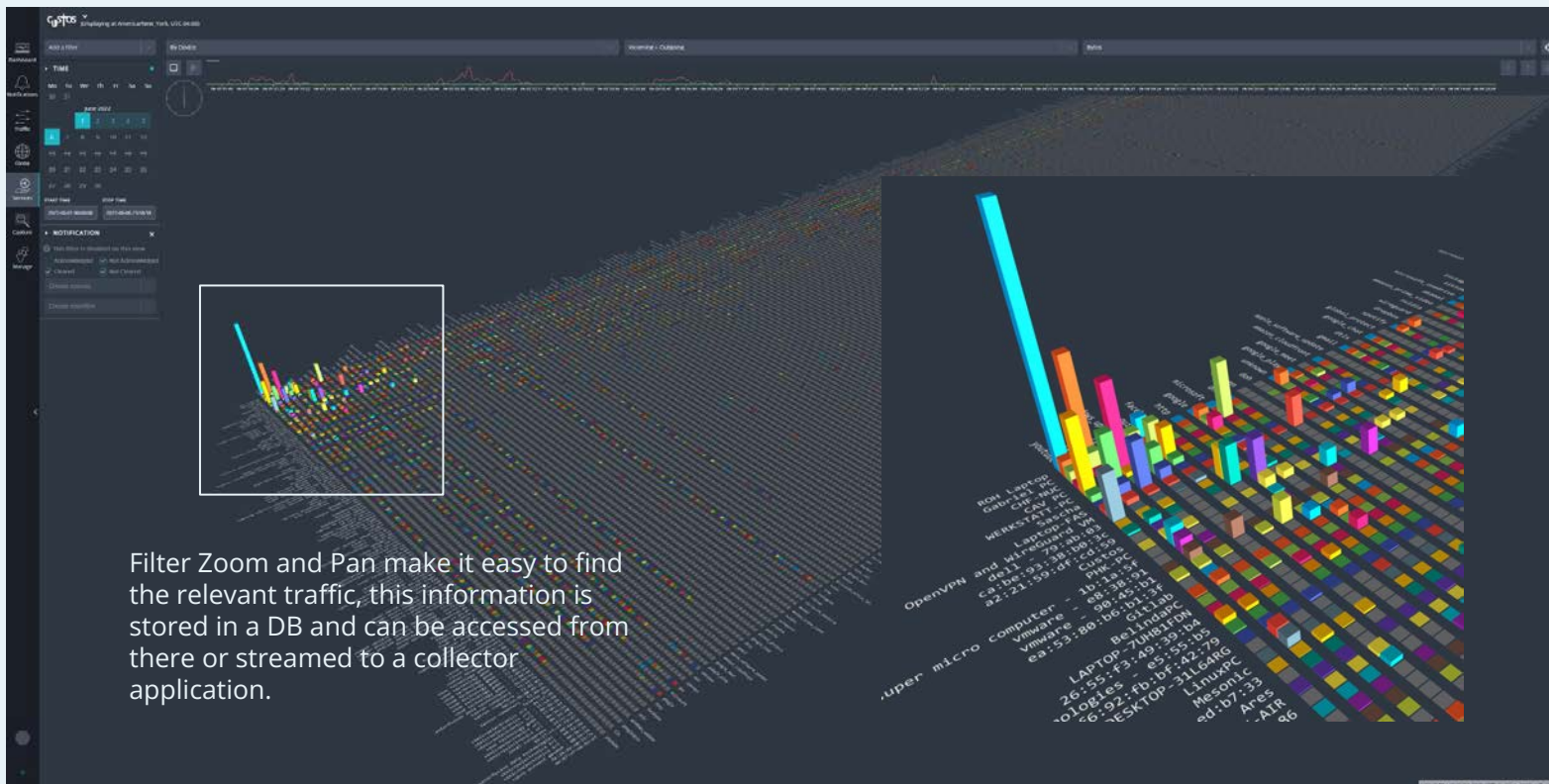
Cubro Metadata enables creating graph, for every individual subscriber:

1. Traffic Volume vs. application in any specific time frame

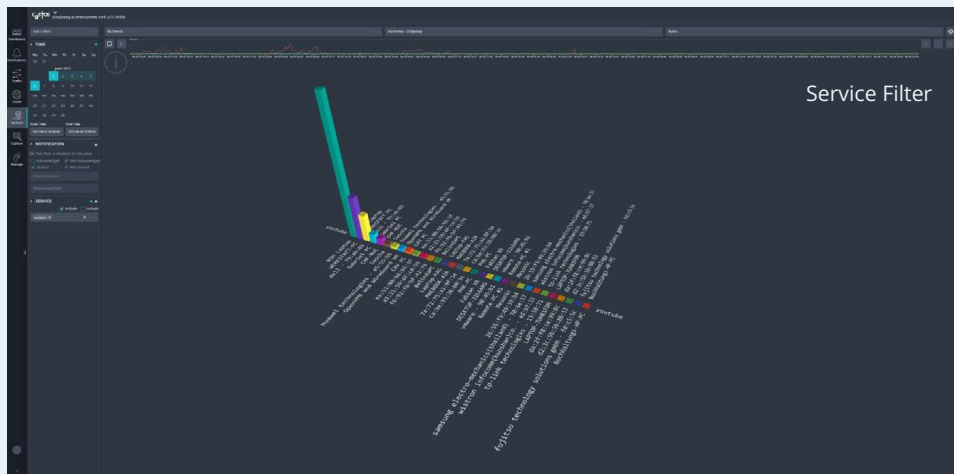
2. Instant Excel export with one click



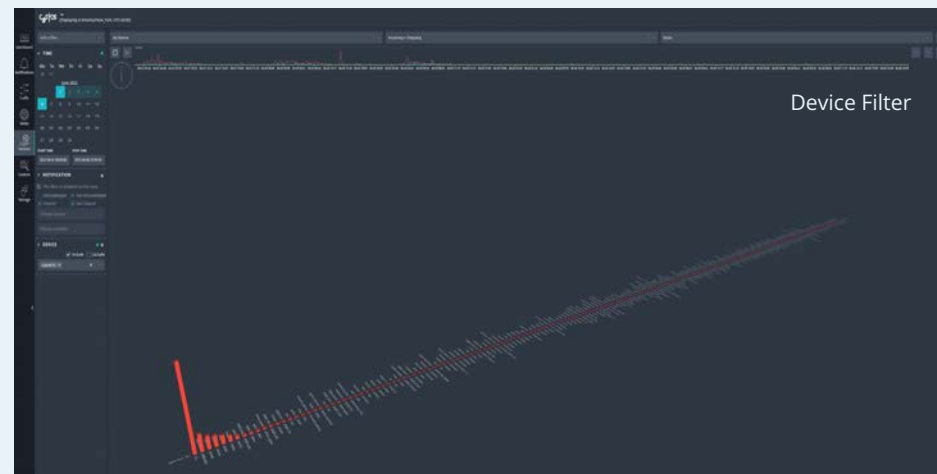
# DPI Service View User vs Application



# Filter option Time/Date – Service - Device

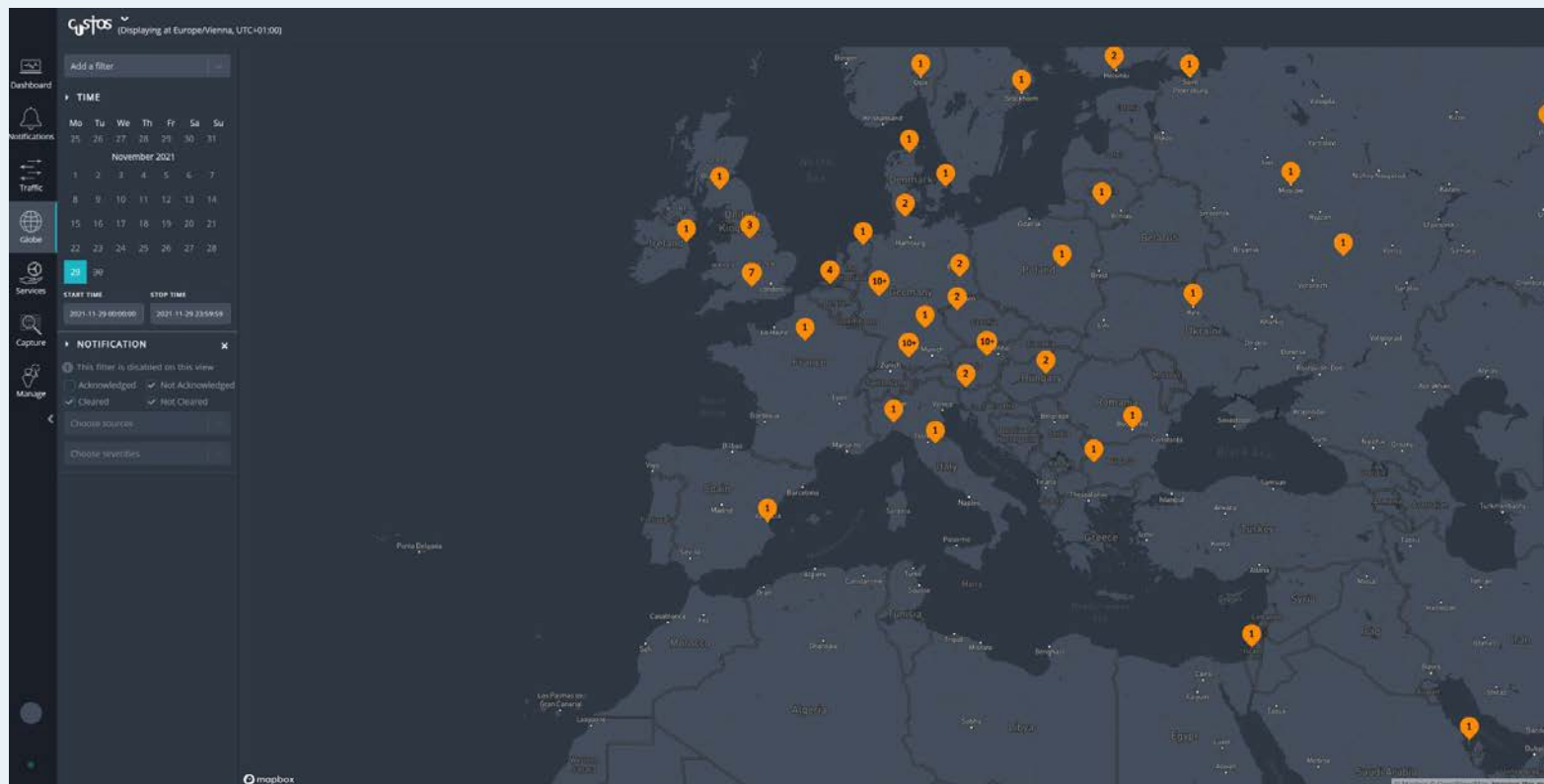


This view shows the traffic of a specific service, over a selected timeframe. It is also possible to select multiple services and exclude specific devices.



This view shows the traffic of a specific device, over a selected timeframe. It is also possible to select multiple devices and exclude specific services.

# Global view



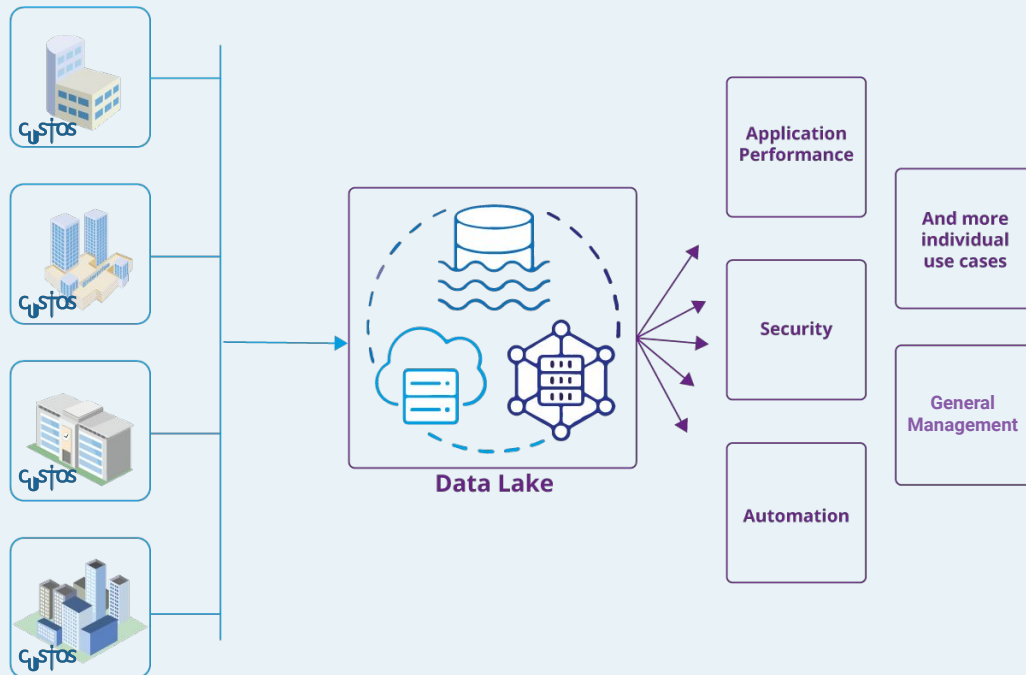
# Monitoring Multi Site, Multi Source Network environments

Custos and Omnishark can serve as metadata feed for multi site solutions.

At each network site, Custos collects raw packets and generates metadata. This metadata is streamed to a central data lake (bronze).

The data lake combines, aggregates, enriches the Custos data with other feeds, like SNMP and logs, offering a comprehensive view.

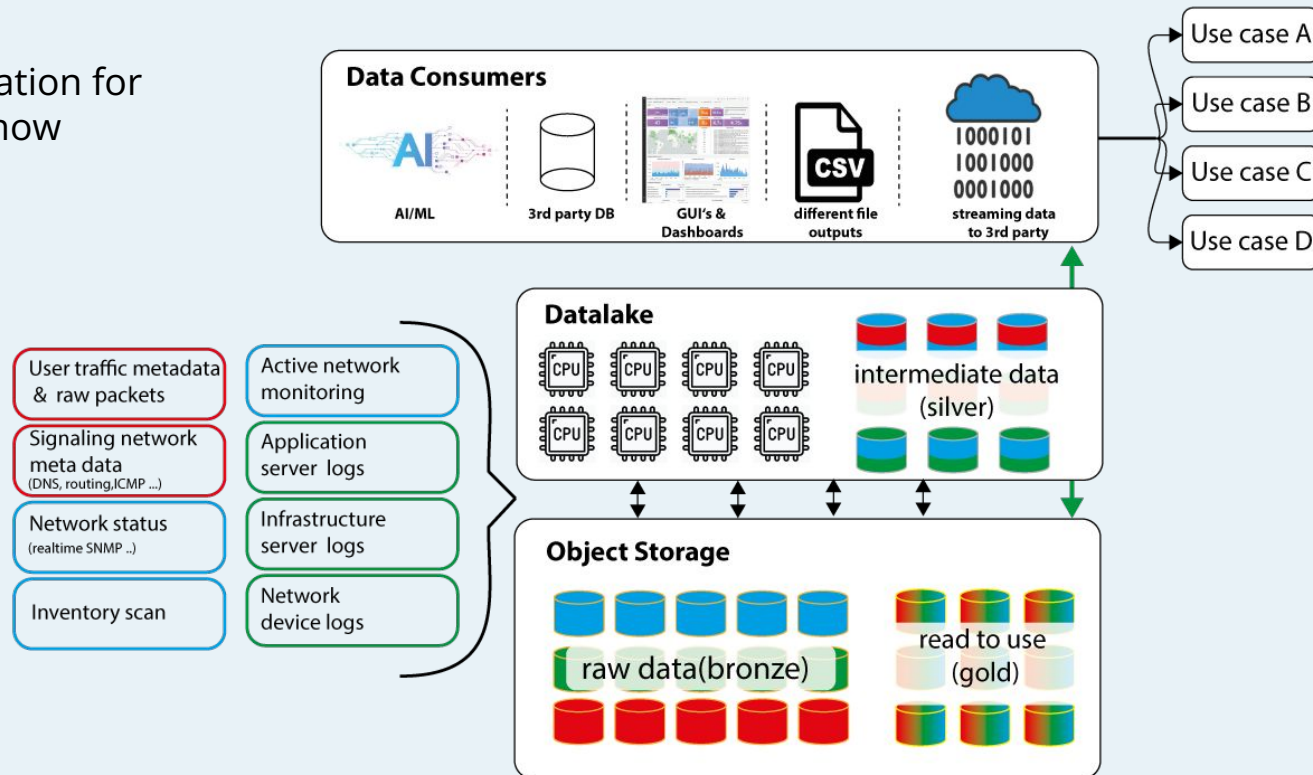
This aggregated data (silver) is then used to generate data to present in use cases (gold).





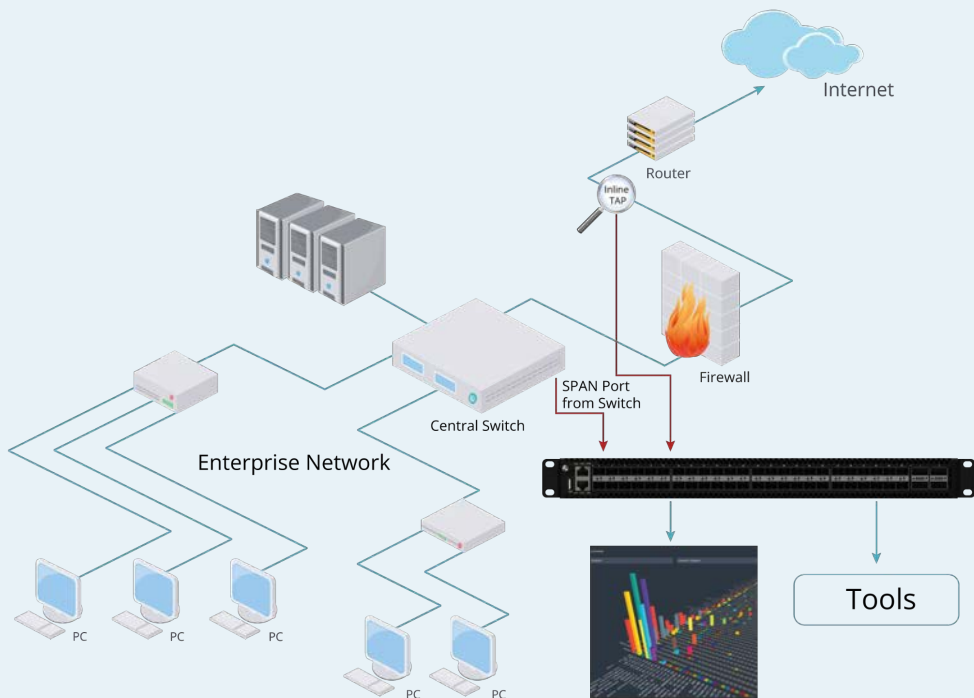
# Custos as Data feed for SIEM and Data lake

Please refer to the presentation for more detailed insight into how Custos can aid in network monitoring.





# Custos Use Cases to Secure Networks



Omnia120 are inline Network appliances which analyze the network traffic to perform security and performance measures.

- Threat Detection & Rolling Capture show known threats by lists
- Find unwanted applications in your network like P2P, Tore, Cryptomining
- Find users with too much traffic volume
- Find new and unwanted devices on your network
- Measure the uplink Bandwidth (did you get what you paid for)
- See strange and unwanted internal traffic misuses of the infrastructure
- See strange and unwanted outgoing traffic misuses of the infrastructure

# Find unwanted applications in your network I/II

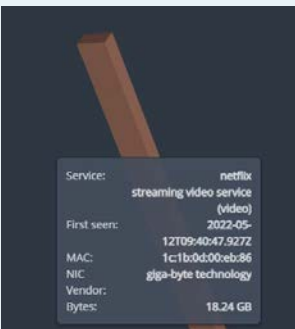
Select a time frame  
(it is possible to select  
timeframes up to  
weeks)

Select the application  
that needs to be  
investigated. It is  
possible to select as  
many applications as  
needed.



Timeline – this  
feature helps to see  
the time when  
the traffic was  
produced.

User / IP / MAC  
identification



Mouseover the bar to  
see the traffic that is  
transported in the  
selected time frame.



# Find users and application/service with the most traffic volume

It is simple to perform this task. Just select the time frame you want to monitor.

Custos automatically sorts the user and the application by volume.

In the left corner you see the top talkers and the top applications.





# Find new and unwanted devices on your network I/II

## Active Network Security Solutions by Custos

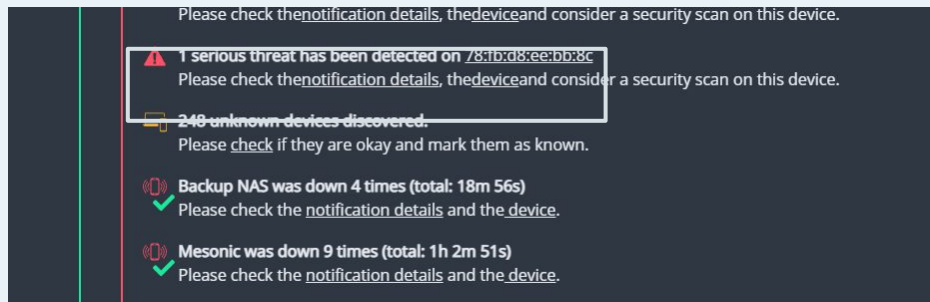
Addressing the Threat of Illegal Connected Devices by continuous Network Scanning by Custos:

- Custos performs constant network scanning.
- It strives to retrieve comprehensive information from all devices (see next slide).



## Online Device Monitoring and Reporting:

- Custos can also check the status of online devices and report this on the dashboard.



# Find new and unwanted devices on your network II/II

The device window shows all devices detected on the network segment.

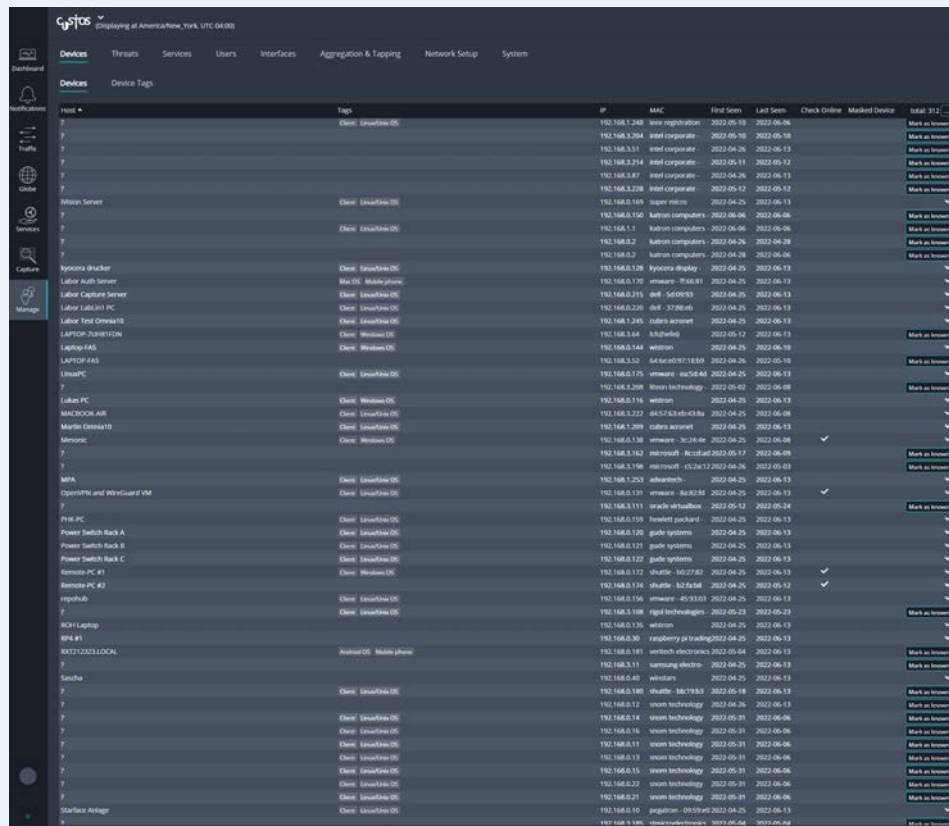
- IP
- MAC
- Device Vendor
- First Seen
- Last Seen

If possible, it also shows:

- Hostname
- Operating system

Each device can be marked as 'known' to remove it from the unknown list.

And you can add all the information that you need to identify the device manually.



Host	Tags	IP	MAC	First Seen	Last Seen	Check Online	Marked Device	Total
192.168.1.248	Intel Linux(OS)	192.168.1.248	Intel corporate	2022-05-10	2022-06-06		Mark as known	1
192.168.1.249	Intel corporate	192.168.1.249	Intel corporate	2022-05-10	2022-06-06		Mark as known	1
192.168.1.251	Intel corporate	192.168.1.251	Intel corporate	2022-05-10	2022-06-13		Mark as known	1
192.168.1.254	Intel corporate	192.168.1.254	Intel corporate	2022-05-11	2022-06-13		Mark as known	1
192.168.1.87	Intel corporate	192.168.1.87	Intel corporate	2022-06-26	2022-06-13		Mark as known	1
192.168.1.238	Intel corporate	192.168.1.238	Intel corporate	2022-05-12	2022-05-12		Mark as known	1
192.168.1.169	super micro	192.168.1.169	super micro	2022-06-25	2022-06-13		Mark as known	1
192.168.1.192	Katron computers	192.168.1.192	Katron computers	2022-06-06	2022-06-06		Mark as known	1
192.168.1.1	Katron computers	192.168.1.1	Katron computers	2022-06-06	2022-06-06		Mark as known	1
192.168.0.2	Katron computers	192.168.0.2	Katron computers	2022-06-26	2022-06-28		Mark as known	1
192.168.0.3	Katron computers	192.168.0.3	Katron computers	2022-06-28	2022-06-06		Mark as known	1
192.168.0.128	Iyosena display	192.168.0.128	Iyosena display	2022-06-25	2022-06-13		Mark as known	1
192.168.0.170	vmware	192.168.0.170	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.215	vmware	192.168.0.215	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.220	vmware	192.168.0.220	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.245	vmware	192.168.1.245	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.64	vmware	192.168.1.64	vmware	2022-05-12	2022-06-13		Mark as known	1
192.168.1.144	vmware	192.168.1.144	vmware	2022-06-25	2022-06-10		Mark as known	1
192.168.1.52	vmware	192.168.1.52	vmware	2022-06-25	2022-05-10		Mark as known	1
192.168.1.175	vmware	192.168.1.175	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.208	vmware	192.168.1.208	vmware	2022-06-25	2022-06-10		Mark as known	1
192.168.1.116	vmware	192.168.1.116	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.222	vmware	192.168.1.222	vmware	2022-06-25	2022-06-08		Mark as known	1
192.168.1.209	vmware	192.168.1.209	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.138	vmware	192.168.1.138	vmware	2022-06-25	2022-06-08		Mark as known	1
192.168.1.192	vmware	192.168.1.192	vmware	2022-06-25	2022-06-09		Mark as known	1
192.168.1.198	vmware	192.168.1.198	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.253	vmware	192.168.1.253	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.131	vmware	192.168.0.131	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.111	vmware	192.168.1.111	vmware	2022-05-12	2022-05-24		Mark as known	1
192.168.1.129	vmware	192.168.1.129	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.126	vmware	192.168.1.126	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.121	vmware	192.168.1.121	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.222	vmware	192.168.1.222	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.172	vmware	192.168.0.172	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.174	vmware	192.168.0.174	vmware	2022-06-25	2022-05-12		Mark as known	1
192.168.1.194	vmware	192.168.1.194	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.198	vmware	192.168.1.198	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.116	vmware	192.168.1.116	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.30	vmware	192.168.0.30	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.181	vmware	192.168.0.181	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.11	vmware	192.168.1.11	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.43	vmware	192.168.0.43	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.190	vmware	192.168.1.190	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.12	vmware	192.168.0.12	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.14	vmware	192.168.0.14	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.16	vmware	192.168.0.16	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.11	vmware	192.168.0.11	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.13	vmware	192.168.0.13	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.21	vmware	192.168.0.21	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.21	vmware	192.168.0.21	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.0.19	vmware	192.168.0.19	vmware	2022-06-25	2022-06-13		Mark as known	1
192.168.1.146	vmware	192.168.1.146	vmware	2022-06-25	2022-06-13		Mark as known	1



click to set label

☒ Known Device  
☐ Check Online Status  
☐ This MAC address marks multiple devices (Router, VMware Host, ...)

COMMENT  
click to set comment

TAGS  
Click to set tags

HOSTNAME  
Click to set hostname

OPERATING SYSTEM  
Click to set operating system

FIRST SEEN  
2022-05-10 06:08:10

LAST SEEN  
2022-06-06 01:36:44

MAC ADDRESS  
70:83:05:01:ad:0a

MAC ADDRESS (VENDOR)  
vmware registration authority - 01:ad:0a

IP ADDRESS(es)  
192.168.1.248  
192.168.1.144

In this menu, you can force Custos to check constantly a device. If the device becomes offline, you get an alarm on the dashboard.

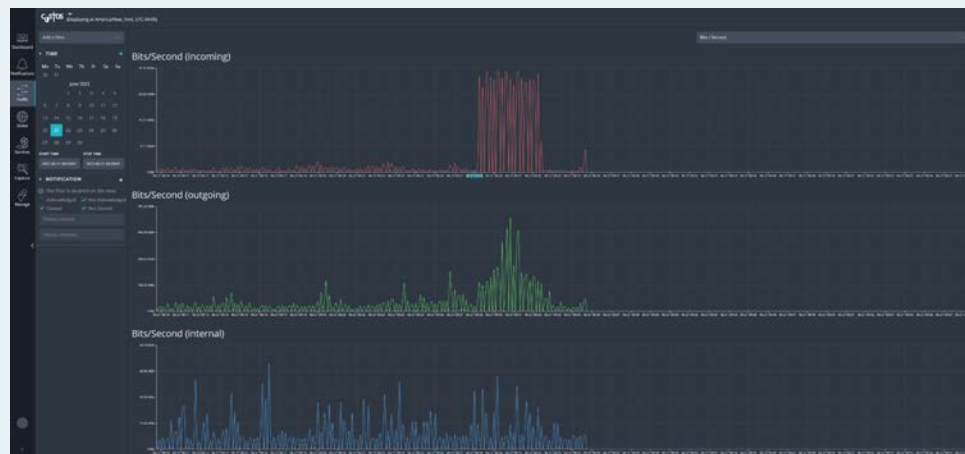
# Measure the uplink Bandwidth

## Ensuring value for your investment



The traffic application shows the live traffic, but you can go back in time to see traffic volume days or weeks ago.

You see three different graphs – outgoing / incoming / internal traffic, and you can select bit/s byte/s and packet/s.



# See strange and unwanted outgoing traffic I/II

Excessive outgoing traffic can have serious implications, potentially involving criminal activity. In the worst-case scenario, it can cause harm to the company and its management.



Typically, there is an 80/20 ratio between incoming and outgoing traffic. If you observe a different ratio without a valid explanation (such as backup operations), it indicates a potential issue.

Your infrastructure can be utilized for Peer-to-Peer (P2P) traffic, suggesting the possible distribution of illegal content from your location. With Custos, you can track the timing and endpoint within your network responsible for uploading this traffic.

The advantage is that it doesn't require deep analytics. A simple glance allows you to understand the ongoing situation.



If you see unusual traffic volume distribution **outgoing** / **incoming** or **internal** traffic, investigate this. Massive uploads may explain it, but such traffic is very rare. Prolonged occurrence indicates a problem.

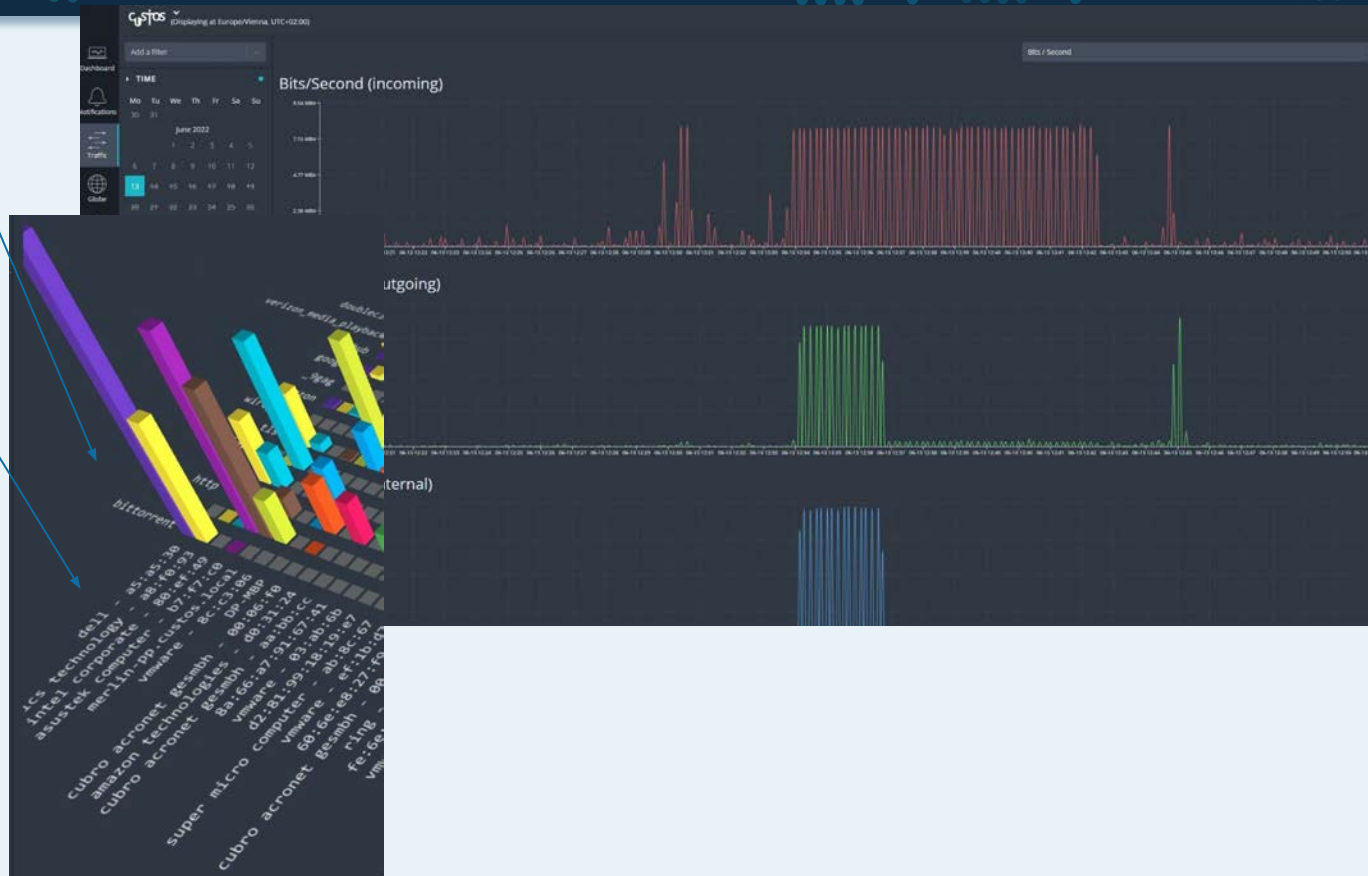
# See strange and unwanted outgoing traffic II/II

This is a common traffic pattern observed in P2P applications like BitTorrent.

In P2P, incoming traffic represents data downloads from the P2P server, while outgoing traffic involves data sharing with user servers on the internet (illustrating the P2P concept).

When multiple P2P servers exist within your network, internal traffic is also present in similar proportions.

Custos' Service View feature can identify the specific device associated with this traffic pattern.





# Safeguarding public Wi-Fi environment

Unwanted traffic poses a significant challenge in various public Wi-Fi environments such as hotels, schools, and coffee shops. It can become a major issue for the owners of these infrastructures. In worst-case scenarios, if criminals exploit the network, the infrastructure owner may face prosecution. Proving innocence without proper tools like Custos can be extremely difficult.

Custos serves as the solution by acting as a logbook, recording the origin, timing, and frequency of network traffic. This allows the infrastructure owner to provide concrete evidence that the traffic originated from the open Wi-Fi and demonstrate when and how frequently it occurred.

This single use case demonstrates the value of investing in Custos, as it provides a cost-effective solution that quickly pays for itself by safeguarding infrastructure owners from potential legal implications.

**Custos is a plug and play Network fire extinguisher**



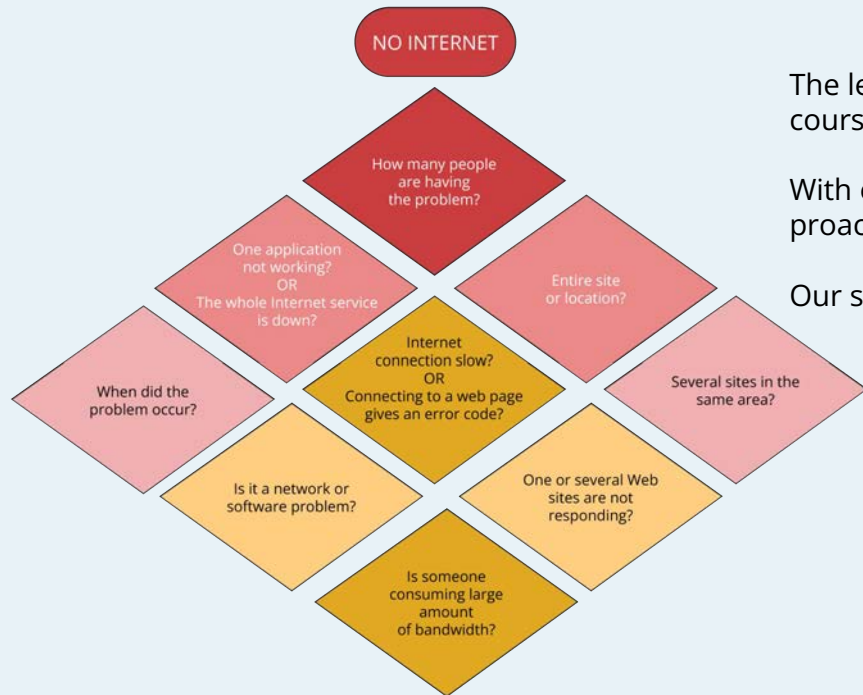
# Mitigating risk in public Wi-Fi environment



Unwanted user issues in public Wi-Fi settings (hotels, schools, coffee shops) pose significant challenges for infrastructure owners. Criminal exploitation of such networks can result in potential legal repercussions. It will be difficult to establish guilt without appropriate evidence provided by a tool like Custos.

Custos, with its comprehensive logging capabilities, accurately records user traffic details, including the source, timing, and frequency. This empowers infrastructure owners to demonstrate the origins of unauthorized access and present compelling evidence regarding the occurrence and frequency of such incidents.

This compelling use case exemplifies the immediate and substantial return on investment achieved by implementing Custos. By ensuring a secure Wi-Fi environment and offering the means to substantiate innocence in critical situations, Custos turns out to be a cost-effective solution for infrastructure owners.



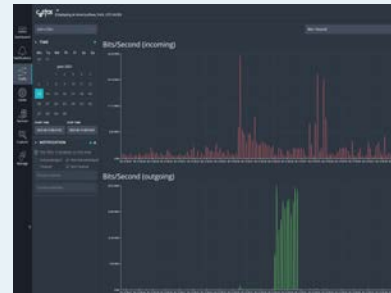
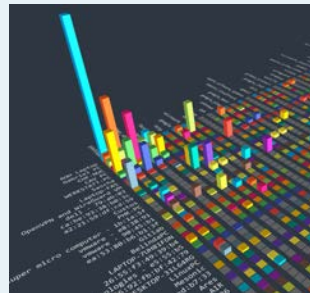
## Streamlining actionable insights and making proactive decision with Custos

The left illustration shows a series of questions that would lead to a useful course of action in case a user has no internet connection.

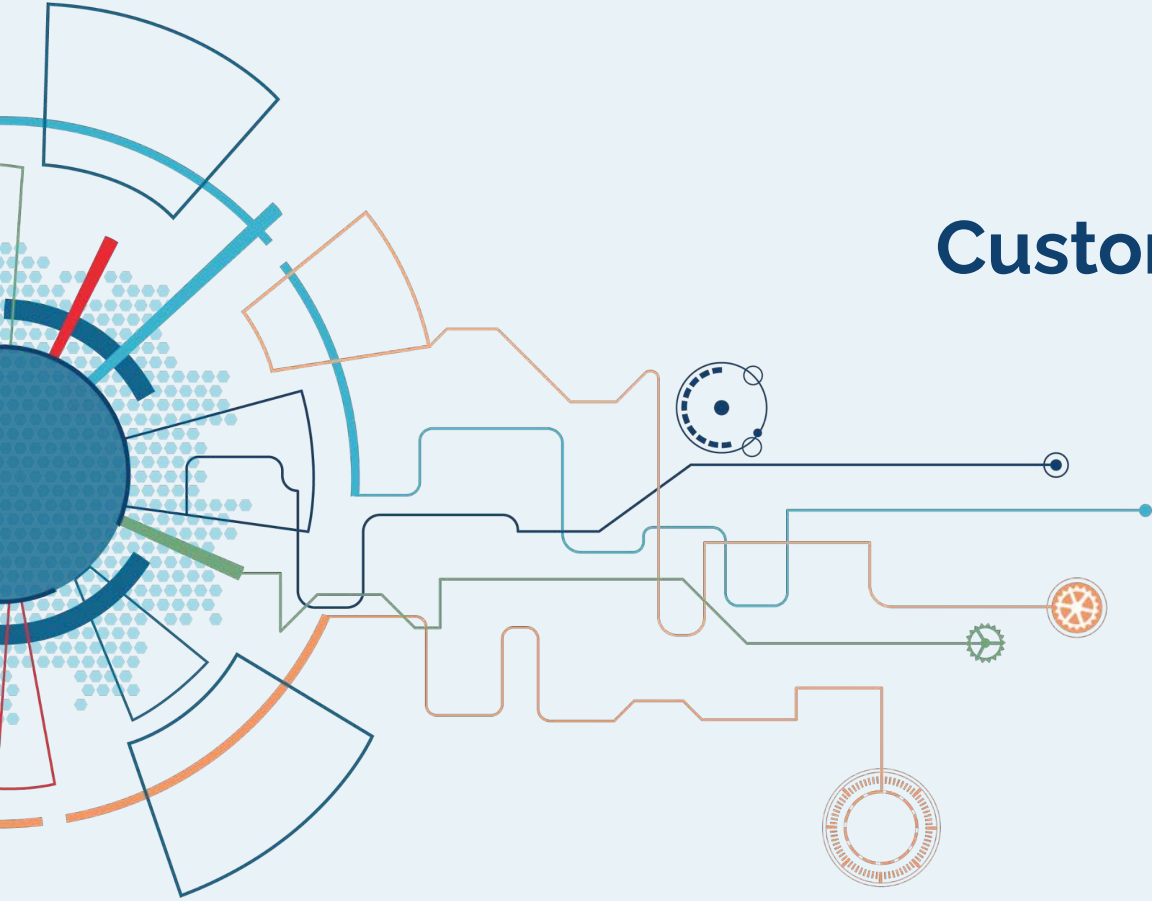
With existing tools, this is difficult to quickly assess and certainly not proactively.

Our solution with Custos can instantly address key questions.

### Two views and you can answer all the questions



# Customer Inquiries



## Wireshark vs Custos

- Capture tool with statistical capabilities
- Not designed for continuous operation
- Requires a performant server for midsize networks (250 Mbit/s and up)
- Lack of rolling capture and capture index makes finding and exporting relevant traffic challenging and performance-consuming
- Works on a single interface, necessitating a TAP and Aggregator or a SPAN port from a switch for bidirectional traffic visibility

- Statistical tool with capture features
- Designed for continuous operation
- Offers a plug-and-play solution with Omnia120 for seamless integration
- Supports midsize networks with efficient performance
- Provides comprehensive statistical analysis alongside capturing functionality
- Enables easy identification and export of relevant traffic
- Offers bidirectional traffic visibility without additional hardware requirements



# Why can my router not do the same?

Many routers or firewalls have monitoring features, but these are primarily intended for troubleshooting purposes rather than comprehensive network monitoring.

- Limited hardware resources: These devices often lack sufficient resources for dedicated monitoring purposes.
- Not designed for continuous monitoring: Monitoring capabilities are typically limited to occasional troubleshooting scenarios.
- Limited packet capture capacity: While capture might be possible, the capacity is usually limited to a few thousand packets.
- Lack of Deep Packet Inspection (DPI): Router/firewall monitoring features generally do not include DPI functionality.

# Can't I use a free software on a server?

Using free software is indeed possible, but similar issues to Wireshark may arise. Free software versions often have limitations and lack support, making them unsuitable for professional environments.

Challenges with free software:

- Limited capabilities: Free versions frequently offer restricted functionalities.
- Lack of support: The absence of support can be a significant drawback in professional settings.
- Limited options for fully free DPI: Finding a fully free Deep Packet Inspection (DPI) version that rivals Custos' features is difficult.



We have operations in all time zones.  
Reach us at: [support@cubro.com](mailto:support@cubro.com)