**JOINT SOLUTION BRIEF**

# Enhance SecOps with enriched network data

### Solution Overview

Together Witfoo and Cubro help security teams collect and centralize high fidelity data for security incident detection and response

### Components

- Omnia120 Advanced Network Packet Broker
- NetFlow Optimizer
- Witfoo Precinct

### Benefits

- DPI-enhanced IPFIX identifies protocols and applications
- Compress flow records to significantly reduce the volume of data exported and stored without losing data granularity
- Enrich flow data with hostname, user identity, and threat intelligence
- Centralize security information and event management in one system that allows for detection, identification, investigation, and remediation of threats leveraging *all* available log sources including syslog, NetFlow, endpoint logs and API integrations

## Introduction

The threat landscape now facing today's networks presents an unprecedented level of sophisticated, well-funded attackers such as APTs (Advanced Persistent Threats), Ransomware as a Service providers, highly-motivated insider threats, and constantly evolving malware.

Simultaneously, networks are becoming increasingly diverse and complex. BYOD, IoT, Cloud, and Containerization are just a few examples of trends and technologies that have contributed to an explosion of nodes and endpoints on the network while blurring the definition of what constitutes the network edge. Not only are attack methodologies evolving but they are doing so while the attack surface expands and the network boundaries become more "porous".

## The Challenge

Security teams face an incredible challenge in staving off ever-increasing numbers of network threats comprised of all levels of sophistication. Compounding this issue is an exponential growth in connected devices and an increasingly decentralized network architecture.

To identify and monitor security events within the network, security operations teams have, and continue, to rely on centralized systems such as SIEMs (Security Information and Event Management). One limitation many SIEMs have is they rely primarily on log data collected from network endpoints. While log data is critical to understanding what is happening on endpoints there are a few things to consider. First, logging must be appropriately configured to be useful, and as devices are rapidly added to expanding networks the potential for configuration errors exist. Second, savvy attackers may also manipulate or remove logs that would otherwise expose their actions. Lastly, endpoint logging is only part of the story; with the addition of network traffic data, the complete picture of a potential threat comes into focus. With more quality data sources, security teams can understand threats holistically and respond to potential incidents more effectively and efficiently.

## Joint Solution

**Omnia120** provides the tapping, aggregation, and flow generation layer by obtaining an out-of-band copy of traffic traversing the network to generate one-to-one IPFIX records. These records contain all information traditionally found in NetFlow as well as protocol and application detection from Cubro's deep packet inspection engine, regardless of whether traffic is encrypted or not. This data is then forwarded to an instance of NetFlow Optimizer for further processing and data enrichment.

**NetFlow Optimizer (NFO)** uses patented streaming technology to aggregate flow records from multiple sources, such as virtual or physical network devices and public cloud flow logs, eliminating redundant data. Simultaneously, the data is augmented with valuable information, including GeoIP data, domain names, VM names, user identity, and threat detection, adding further layers of data enrichment. The output is also standardized to Syslog format before being forwarded to WitFoo Precinct.

**WitFoo Precinct** leverages the enriched output from the Omnia120 and NFO, along with other sources such as syslog, Kafka queues, APIs, agent data (e.g. Beats), and other log sources deployed throughout the infrastructure. Precinct is the centralized console that combines and correlates massive amounts of disparate data into meaningful, investigable units. By crowdsourcing a global community of cybersecurity expertise and leveraging time-tested methodologies from physical law-enforcement, WitFoo enables security teams to efficiently progress through the lifecycle of an attack; from threat detection and identification to analysis, and finally remediation with a robust set of SOAR (Security Orchestration and Automation) capabilities and API integrations with third-party solutions.

## Joint Solution Components

### The Cubro Omnia120 Advanced Network Packet Broker

The Omnia120 is an advanced network packet broker designed from the ground up to address the needs of evolving networks and demanding throughput requirements. Omnia provides purpose-built hardware capable of handling network links from 1 Gbps to several 100 Gbps and a feature-set derived from years of experience and engineering. Omnia combines features included in Advanced Network Packet Brokers with high-performance multi-core CPUs to enable numerous network monitoring, security and analytics uses cases and applications, including those from partners and the open-source community.

### Cubro NetFlow Optimizer

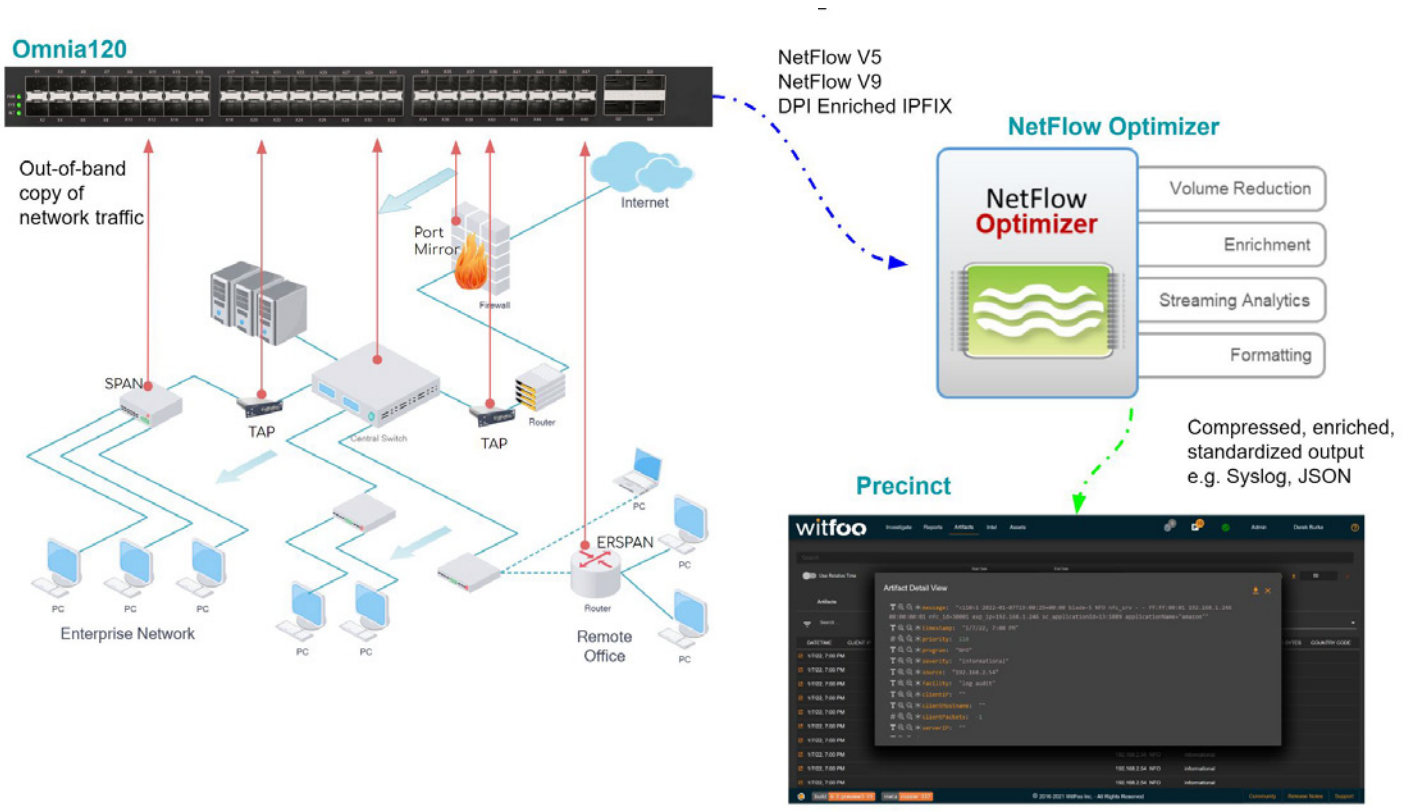
NetFlow Optimizer (NFO) uses patented streaming technology which allows the processing of flow data up to 10 times faster than competitive products. It is complementary to traditional network monitoring and security solutions. NFO provides aggregation of records from multiple flow data sources, converts it into standard Syslog or JSON format, filters to eliminate redundant data and enriches with useful additional information delivering a critical component for complete network visibility.

**WitFoo Precinct**

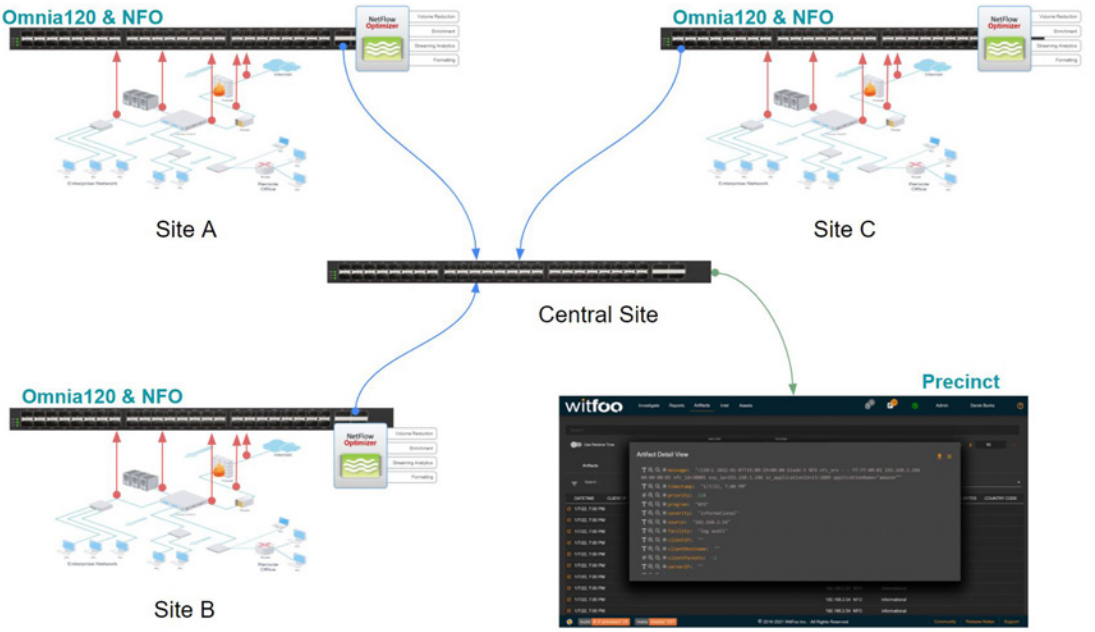
WitFoo Precinct is a Comprehensive Security Operations (SECOPS) Platform built to mature the craft of cybersecurity operations. Leveraging a global community of cybersecurity experts and time-tested approaches from law enforcement, Precinct combines the best capabilities of SIEM, SOAR and Incident Response platforms to deliver meaningful data to everyone from the junior security investigator to the Board of Directors. Coordinating intelligence, expertise, and operations across the craft of cybersecurity operations, WitFoo decreases cybercrime through collaborative enforcement, deterrence and prevention.

## Use Cases

A combination of Cubro TAPs and mirror ports (such as SPAN and ERSPAN feeds) provide a copy of all network traffic to an Omnia120. The Omnia120 generates DPI enriched IPFIX records from all traffic sessions. These records are sent to an instance of NetFlow Optimizer for processing, compression, and further data enrichment. The output is standardized and forwarded to Witfoo Precinct for Security Operations. Additionally, the Omnia 120 can aggregate, filter, and distribute traffic to out-of-band security and monitoring tools (such as an IDS) and NetFlow Optimizer can ingest other structured data, such as public cloud flow logs (AWS/Google VPC Flow logs, Azure NSG Flow logs), for processing and forwarding to Precinct.



As in the example above, a combination of Cubro TAPs and mirror ports (such as SPAN and ERSPAN feeds) provide a copy of all network traffic to an Omnia120. The Omnia120 generates DPI enriched IPFIX records from all traffic sessions. These records are sent to a local instance of NetFlow Optimizer for processing, aggregation, and further data enrichment. The output is standardized and sent to a remote centralized installation of Witfoo Precinct for retention and analysis.




## About WitFoo

Built by veterans of the military, law enforcement and cyber security, WitFoo is dedicated to delivering sustained success to the practitioners of cyber security operations.
Thousands of hours of ongoing research in the trenches with analysts, investigators, managers and executives led to the forming of WitFoo and the subsequent work. Secure together, WitFoo delivers the tools and data that allow for collaborative cybersecurity and prosecution of cyber criminals, resulting in the deterrence and prevention of cyber crime.

## About Cubro

Cubro is a leading vendor of network visibility solutions that include network TAPs, Advanced Network Packet Brokers, Bypass Switches and Network Probes, for Service Providers and private and public sector Enterprises worldwide. Our solutions improve security posture while reducing costs by increasing the effectiveness and lifecycle of network security devices, improving business continuity, and reducing the total cost of ownership (TCO) while increasing the ROI of network security. Cubro's products remove network blind-spots to ensure all relevant network traffic is available for security analysis, filter out unnecessary network traffic, and provide high-availability capabilities for security solutions.

**For more information please visit www.cubro.com, www.witfoo.com**



**Cubro Network Visibility**
EMEA USA APAC Japan
support@cubro.com

**Cubro Network Visibility**
Ghegastraße 3
1030 Vienna, Austria

**Tel.:** +43 1 29826660
**Fax:** +43 1 2982666399
**Email:** support@cubro.com

**Cubro Asia Pacific**
8, Ubi Road 2 #04-12
Zervex
Singapore 408538

**Tel.:** +65-97255386
**Email:** jl@cubro.com


**Cubro North America**
Cubro Network Visibility Inc.
225 Peachtree Street NE,
Suite 1100, Atlanta, GA, 30303, USA

**Email:** americas@cubro.com

**Cubro Japan**
6-7-22, Shinjuku,
Shinjuku,
Tokyo, 160-0022 Japan

**Tel:** +81(0)50-3708-5839
**Email:** japan@cubro.com