SYSTROME

# Seeing the Unseen in Your Network

# UNIVERSAL NETWORK VISUALIZER - UNV

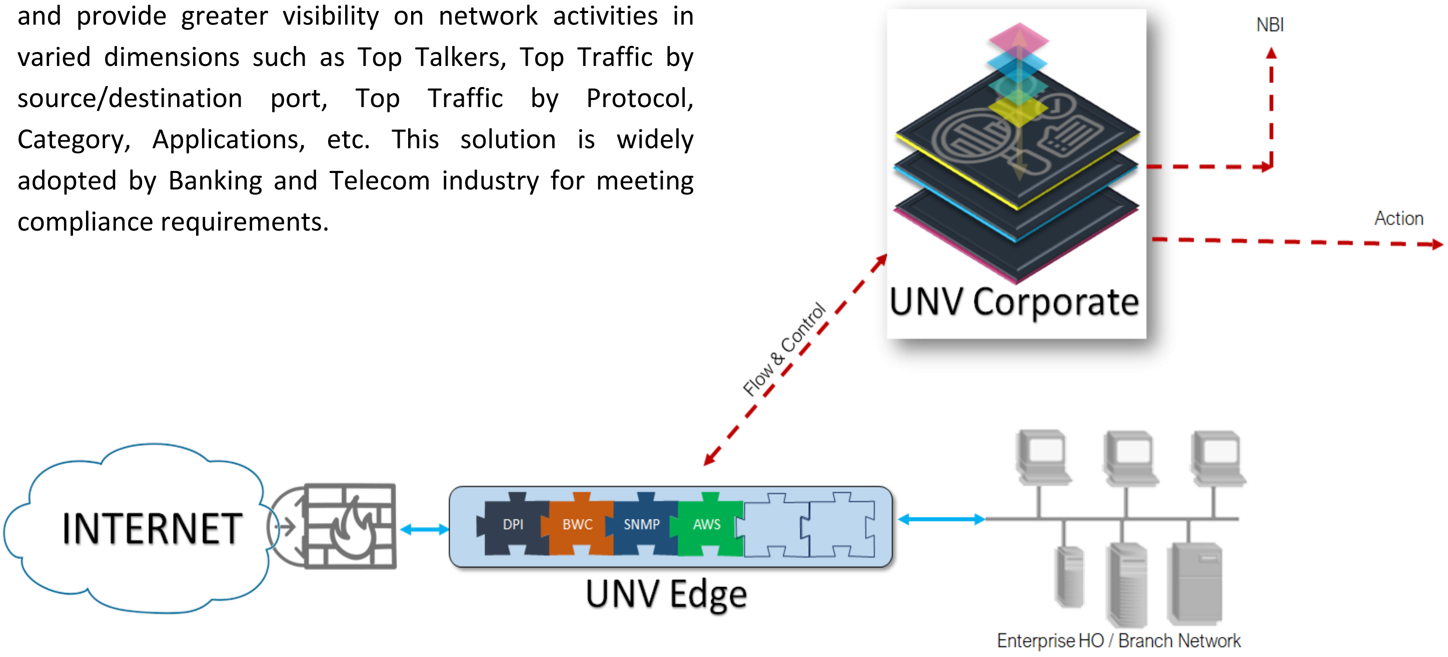
## Product Overview

Universal Network Visualizer collects the comprehensive real-time analysis data from UNV edge device which are deployed just before your gateway as an in-line transparent bridge device or installed in a monitoring port of a switch to gather, analyse and report to UNV Corporate - a centralized data lake for analysis and reporting. With Aheesa’s SPADE Engine the UNV Edge is capable of having multiple Agents which can not only have a deep packet inspection and traffic throttling or shaping it can also have proactive monitoring of multiple Network elements and report status to the UNV Corporate for further analysis and reporting.

Systrome’ s UNV captures packet level network traffic generated by users, systems and applications to dissect and provide greater visibility on network activities in varied dimensions such as Top Talkers, Top Traffic by source/destination port, Top Traffic by Protocol, Category, Applications, etc. This solution is widely adopted by Banking and Telecom industry for meeting compliance requirements.

Systrome’ s UNV follows a streamlined process to group and classify network assets. Assets are tagged at Agent, Organization and Branch levels. Based on the organization's requirements, different edge agents are initiated to capture the required network/system data. The built-in access control and authorization module restricts users based on their roles and priorities (User, Admin, Super Admin).

Systrome’ s UNV can Scale for 100,000's of devices segmented across federated hierarchy also provide plug-in support to capture data from discrete services and delivers Faster search and querying with underlying Elastic Search infrastructure.



## Universal network visualizer Components:

UNV follows the streamline process to group & classify the data. Also, tagging of assets at Organization & Branch level. Defining the agent and asset type as per the requirement of the organization. User can also define access controls at different level and priorities (User, Admin, Super Admin). Systrome’ s UNV can Scale for 100,000's of devices segmented across federated hierarchy also provide plug-in support to capture data from discrete services and delivers Faster search and querying with underlying Elastic Search infrastructure

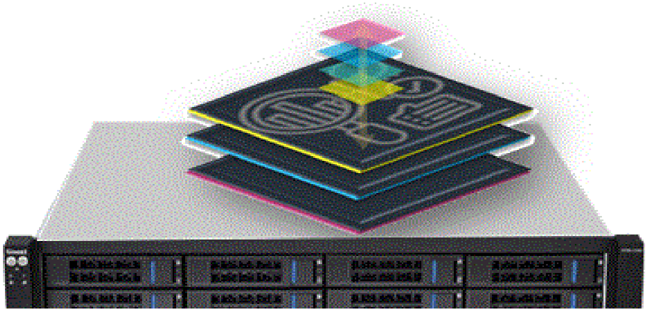
UNV Corporate: An Analytical server, collecting all the information from various Collection points (UNV Edge) and used for deep analyses, reporting and alarming.

UNV Corporate allows organizations to discover deep, unique insights from their data through augmented analytics across the enterprise network. Provide self-service analytics that enables users to build compelling visual stories and to confidently make highly informed decisions. Allow to Manage 1000s of UNV Edges from a single UNV Corporate and create a compiled traffic information and status.

Creating an easier path to insights while performing more in-depth and impactful data analysis. Providing a holistic approach from start to finish, UNV Corporate streamlines data discovery and self-service analytics to maximize efficiency of your network, application and security. With a High Storage support from 2TB to 64TB or more storage allow to maintain long historical data.

UNV Edge Device: Hardware appliance of various capacities coming from lower to higher end specifications, suitable for branches to an enterprise datacentre or a service provider network

Systrome’ s Universal Network Visualizer offers a special type of network asset located in branches that collects, aggregates, analyses and perform intermediate actions to improve response and reduce latency. Edge transmits the data to cloud for deeper analysis and actions. Edge runs one or many agents as per need. These agents control and manages Sensor, Network Assets and Edge.



UNV - Edge Agents:

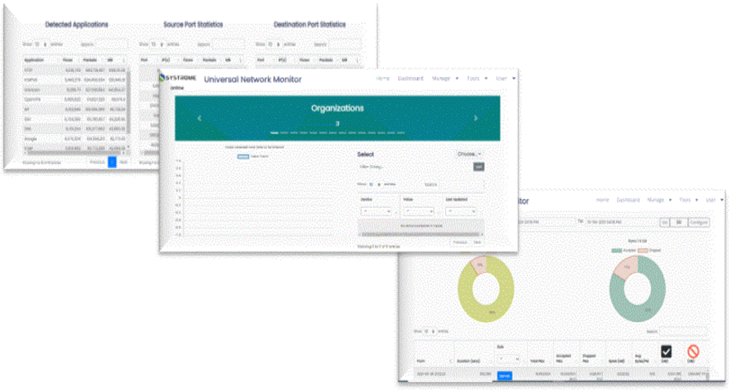
A collection of software modules loaded in UNV Edge for various purpose including traffic collection, Deep Packet Inspection, Authentication, SNMP and much more.

Systrome’ s Universal Network Visualizer offers a special type of network asset located in branches that collects, aggregates, analyses and perform intermediate actions to improve response and reduce latency. Edge runs one or many agents as per need. These agents control and manages Sensor, Network Assets and Edge.

Deep Packet Inspection Agent – Deep packet inspection (DPI) provides 100% visibility over the network by transforming the raw data into a readable format and enabling network and security managers drill down to the minutest details of the packet transmitted.

Bandwidth Throttling and Control Agent - Systrome’ s UNV can fully identify common Internet applications, such as P2P download, IM instant messaging, online video, stocks, games and so on, which often results in Internet bandwidth abuse. By deploying Bandwidth throttling and management, users can effectively curb various applications snatch valuable bandwidth and IT resources, thereby ensuring the rational allocation and quality of business-critical network resources, overall performance

Device’s discovery and asset management (SNMP Agent)- SNMP is adequate as a sensor for threshold-based volumetric attack detection and allows automated redirection of Internet traffic through cloud scrubbing centres when under attack. By automating the process of detection, mitigation time can considerably be reduced and volumetric attacks mitigated through on-demand cloud DDoS services. SNMP provides minimal impact on the device’s configuration and works with pretty much any network device and vendor. Systrome’ s UNV can configured to receive all traps from multiple end devices and the data can be grouped and classified for deeper insights and analysis.



## UNV Features:

### Real - Time Network Traffic Analysis:

Systrome’ s UNV provides in-depth insights into type of traffic/network packets or data flowing through organizations network. Consolidated reports provide overall traffic statistics for each WAN link. Using UNV for analysis, administrators can have a look into current traffic patterns along with details on hosts, applications, and conversations generating traffic. UNV admins can also analyses network traffic trends to identify link utilization metrics, peak usage hours, and more. UNV does perform in-depth network packet analysis to give you a deeper and holistic view of protocol, application usage, and other utilization trends.

Not only admins could view reports ranging from the last few minutes to the last quarter, UNV allows to custom select the time period for that they want to review their network traffic patterns and export the reports to CSV or PDF as required.

### Real -Time Risk Flow analysis:

Systrome’ s UNV helps to keep a close watch on network. In the recent years network threats and ransomware activities are becoming more common and hence, real-time network monitoring is really critical to identify attacks via insecure protocols and open risks. UNV shares valuable insights and provides an overview for any suspicious activity associated within management protocols. UNV provides a typical enterprise with better insights on threats, applications and risks associated in their network beyond just the end points. With the rise in the mobile devices, IOT devices, Smart TV’s etc., network monitoring needs to be intelligent and not just the logs from firewall

Creating an easier path to insights while performing more in-depth and impactful data analysis. Providing a holistic approach from start to finish, UNV Corporate streamlines data discovery and self-service analytics to maximize efficiency of your network, application and security.

### Historic Data & Incident Analysis:

Historical data is critical to analysing past events & records. Many tools for monitoring network traffic don’t retain the data as time goes on, however Systrome’ s UNV keeps the historical data in place and you can fetch the records as per customer’s requirement.

UNV stores and presents historical data for a group based on time period to display in query-based views (chart views, table view, and the topology view). Keeping historical network performance data digitally inline helps organizations to quickly determine current network issues by comparing it to problems previously detected.

### Simple Configuration & Management:

Systrome’ s UNV supports centralized management, reporting and analysis to provide deeper insights for implementing controls based on users’ requirements within the threshold of management policies. Network Management is no longer limited to managing device(s) and monitoring logs inside a corporate. A holistic approach is required to Secure, Protect and Defend against external threats. UNV is an open standard platform with customizable features and functionalities with a simple GUI to track, manage, analyses and report network assets and its activities that are deployed across corporates and client services.

## UNV Edge Appliance Specification:

| **Hardware specifications** | **UNV 50A Series** | **UNV 100X Series** | **UNV 500X Series** | **UNV 1000X Series** |
|---|---|---|---|---|
| Processor | ARM Processor | Celeron Processor | Atom Quad core processor | Pentium Processor |
| RAM | 2G | 2G | 4G | 4G |
| Storage | 256 GB | 256 GB | 512 GB | 512 GB |
| Network Interface | 2Ports(2x1Gb RJ45) | 2Ports(2x1Gb RJ45) | 4Ports(2x1Gb RJ45) | 4Ports(2x1Gb RJ45), 1 Management |
| Throughput | 50MB | 100MB | 500MB | 1GB |
| **Hardware specifications** | **UNV 2000X Series** | **UNV 3000X Series** | **UNV 5000 Series** | **UNV 10000 Series** |
| Processor | Xeon Processor | Xeon Processor | Dual Xeon Processor | Dual Xeon Processor |
| RAM | 32 GB | 32 GB | 64 GB | 128 GB |
| Storage | 1 TB | 1 TB | 1 TB | 1 TB |
| Network Interface | 6Ports (2x10Gb SFP+, 4x1Gb SFP) | 6Ports(2x10Gb SFP+, 4x1Gb SFP) | 6Ports(2x10Gb , 4x1Gb RJ45) | 4Ports(4x10Gb SFP+) |
| Throughput | 2GB | 3GB | 5GB | 10 GB |
| Reliability | | | | |
| Operating Temperature | 0℃～45℃ | 0℃～45℃ | 0℃～45℃ | 0℃～45℃ |
| Storage temperature | -20℃～70℃ | -20℃～70℃ | -20℃～70℃ | -20℃～70℃ |
| Humidity | 5%-95%, no condensing | 5%-95%, no condensing | 5%-95%, no condensing | 5%-95%, no condensing |

The network management is no longer limited to managing device inside the corporate and holistic approach is required to Secure, Protect and Defend against External threats. UNV is an open standard platform with customizable features and functionalities to keep track, manage, analyse and report for network assets which are deployed across corporates and client services which runs 24*7 across different geo locations via a simple graphical user interface. Also, offers a High Storage support from 2TB to 64TB or more storage allow to maintain long historical data

## KEY HIGHLIGHTS:

- Integrating with existing ticketing system.
- Elastic Queries for ad-hoc reporting and customizations.
- Plug-in support to capture data from discrete services
- SNMP enabled threshold-based attack detection and automated redirection of internet traffic.
- Automating the process of detection, reduction, mitigation in volumetric attacks on services.
- Monitor specifics from databases with customized-configured UNV No-SQL/SQL queries.
- Network Visualization - Application Monitoring - Deep Packet Analysis.
- Detect, alert, block and notify Anomalies and further actions.
- Identify link utilization metrics, peak usage hours, and more.
- Service Discovery, Outage, Analysis and Management.
- Detailed statistics about every application running in network.
- Monitor all types of servers in real time for availability, accessibility, capacity.

## Applications:

### • Service Providers – Multi-tenant Monitoring of services

Service Providers to have multi-tenant monitoring services. As utilization of your user base grows, you may plan for additional devices, services and bandwidth to stay ahead of demand. Actively tracking the status of your devices and software applications means you can understand what is being used at any given time and how your users are consuming their devices and service patterns. Benchmarking your current performance and setting goals and milestones that you need to achieve will enable you to increase performance and stay ahead of the competition

### • Corporate Branch to Branch level Management

Corporates need to have branch wise data management and control to collect comprehensive real-time analysis information. UNV edge device(s) that are distributed and deployed at each network node provides operations staff with vivid and graphical status of every network asset and its activities in the business network. Using deep learning algorithms to analyse patterns with collected data, it can be extended to detect, alert, block and notify anomalies for further actions.

### • SAAS providers for application performance monitoring

SAAS providers are required to have a deep look in to application performance and hacking threats. Hence, a closer watch is required to monitor the operational and performance status of the network. In the recent years network threats and ransomware activities are becoming more common and hence, real-time network monitoring is really critical to identify attacks via insecure protocols and open risks. UNV shares valuable insights and provides an overview for any suspicious activity associated within management protocols. UNV provides a typical enterprise with better insights on threats, applications and risks associated in their network beyond just the end points.

### • BFSI Effective Monitoring & Analysis

Banks should real time monitor server and service utilization and perform data pattern analysis to track any irregular activity happening at a given time. The tell-tale signs of malware having gotten past your security can be as simple as a traffic spike on your system. And if you're not looking in the right place or at the right time, this might go undetected. Having software which can recognize the expected traffic and alert you when it is exceeded is essential if you're going to be confident in the security of your network. On top of this, there are the physical devices in the bank itself: key systems, fire alarms, security cameras, and so on and it requires 24x7 monitoring.

- Datacentres Statistical Monitoring & Policy Management

Datacentres to have complete historical traffic monitoring, auditing and ensure compliance with security policies implemented. Real time datacentre monitoring becomes paramount when organizations want to ensure low downtime and improve the overall performance of your datacentre. However, there are several vital aspects to be monitored, which becomes virtually impossible as the size of the datacentre increases. To ensure the best performance from your datacentre, it is crucial to implement datacentre performance monitoring based on three important parameters - network connectivity, server performance and storage performance. The main setback admins face while executing this, is the lack of an integrated datacentre monitoring solution that provides you visibility over all these three aspects. UNV give you a holistic approach to monitor not only real time data but also the historical data for better understanding of your network.

www.systrome.com
info@systrome.com