

# WireX Network Forensics Platform

Datasheet

## From Suspicion to Facts in Minutes





Organisations today are under constant pressure to identify successful attacks and respond quickly in order to minimise damage. The struggle with lack of context, ineffective tools and even the skills to properly investigate is at the heart of the problem. Wirex Network Forensics Platform (NFP) engages your entire SOC team to conduct dramatically faster, better investigations while chopping down data retention costs.

When a malicious activity is detected, Wirex NFP has a unique approach to compile and analyse extensive data into clear and comprehensive intelligence critical for the investigation. The solution also enriches this data using external threat feeds, while managing and documenting the investigation workflow.

To overcome forensics limitations and complexities, Wirex NFP automates analysis efforts so that security professionals at all levels, i.e. Security managers, SOC operators, analysts and incident response teams—can make faster and more informed decisions based on the actual content of network conversations, rather than just the metadata.

Wirex NFP sensors continuously monitor all parts of the enterprise network, translate it into content and behaviour-aware intelligence that can be immediately understood and provide a fast and intuitive interface for querying and researching network-born activities.

## Solutions Benefits

			
<p><b>Gain Complete Visibility</b></p> <p>Clear and immediate understanding of user behaviors and application content across the enterprise network</p>	<p><b>Remove Skill-Set Barriers</b></p> <p>Empower the entire team with the ability to quickly validate alerts, handle complex investigations and escalate fewer tickets</p>	<p><b>Boost Forensics History</b></p> <p>Up to 25X longer retention periods with greater context and visibility over traditional forensics solutions</p>	<p><b>Accelerate SOC and IR Processes</b></p> <p>Eliminates the heavy lifting of data analysis and automates security investigation and response procedures</p>

## Contextual Capture

WireX's groundbreaking technology eliminates the need to store raw packets by reconstructing the entire OSI stack, continuously extracting application contents and uncovering user behaviours:

- Full stack behavioural analysis, classifies the user actions performed within each application
- Real-time reconstruction and extraction of application contents, such as file transfers, emails, chats, DB transactions, authentications, as well as remote desktop sessions
- Customisable analysis modules to provide the same level of visibility into proprietary business applications, as it does for enterprise applications

## Powerful Monitoring & Federated Analytics

Distributed architecture designed to deliver true sustainable visibility into 100Gbps networks:

- High performance database, optimised for large deployments
- Scalable capacity to store many months of complete intelligence
- Advanced filtering capabilities for analysing and/or capturing traffic selectively
- Intuitive query language enables powerful retrieval of relevant data, without wasting precious time on manual examination of network packets and sessions
- Centralised management for a secure, single point of view, allowing multi-site and multi-sensor investigations

## Forensics & Response Framework

Streamline your forensics processes with adaptive and easy to use investigation tools that allow security professionals at all levels to handle security incidents quickly and effectively:

- Integration with the existing security infrastructure, such as leading SIEM solutions and data enrichment tools—host and IP reputation, Sandbox, etc.
- Built-in case management to support the entire investigation life-cycle
- Investigation playbook modelling capabilities, support collaboration across team members

Specifications		WNFP-M2000	WNFP-M4000	WNFP-M6000	WNFP-M10000	Central Management
Analysis Rate		2 Gbps	4 Gbps	6 Gbps	10 Gbps	N/A
Monitoring Rate		20 Gbps	40 Gbps	80 Gbps	120 Gbps	N/A
Interfaces		4 x 10/100/1000 4 x 10 GbE	8 x 10/100/1000 8 x 10 GbE	12 x 10/100/1000 12 x 10 GbE 4 x 40 GbE	24 x 10/10/1000 24 x 10 GbE * 6 x 40 GbE * 4 x 100 GbE	2 x 10/100/1000
Form Factor		2U	2U	2U	4U	1U Half-depth
Storage		20TB	40TB	40TB	150TB	1TB
Storage Extensions		80TB	200TB	300TB *	500TB *	N/A

\* More options available

Leading enterprises choose WireX Systems as a key component in their security infrastructure to accelerate incident response, mitigate data theft and simplify responding to the magnitude of security alerts they must act on every day.

