Datasheet

WireX Systems Ne2ition Threat Detection & Response

Turbocharge Your Response

Organizations today are under constant pressure to identify successful attacks and respond quickly in order to minimize damage. The struggle with a lack of context, ineffective tools, and even the skills to properly investigate is at the heart of the problem. WireX Systems NDR Platform delivers security teams with complete network visibility and powerful tools to streamline investigation processes.

When a malicious activity is detected, WireX Systems Platform has a unique approach to compile and analyze 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 entire investigation workflow.

To overcome forensics limitations and complexities, WireX Systems 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 Systems sensors continuously monitor all parts of the enterprise network, translate it into content and behavior-aware intelligence that can be immediately understood, and provide a fast and intuitive interface for querying and researching network-born activities.

Solution Benefits

Remove Skill-Set Barriers

Empower the entire team with the ability to quickly validate alerts, handle complex investigations and escalate fewer tickets

Gain Complete Visibility

Clear and immediate understanding of user behaviors and application content across the enterprise network

Boost Forensics History

Up to 25X longer retention periods with greater context and visibility over traditional forensics solutions

Accelerate SOC and IR Processes

Eliminates the heavy lifting of data analysis and automates security investigation and response procedures

Copyright @ 2023 WireX Systems. All Rights Reserved

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 behaviors:

- Full stack behavioral 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
- Customizable analysis plugins to extend common enterprise applications visibility and support home grown and proprietary business applications

Massive-Scale Monitoring & Analytics

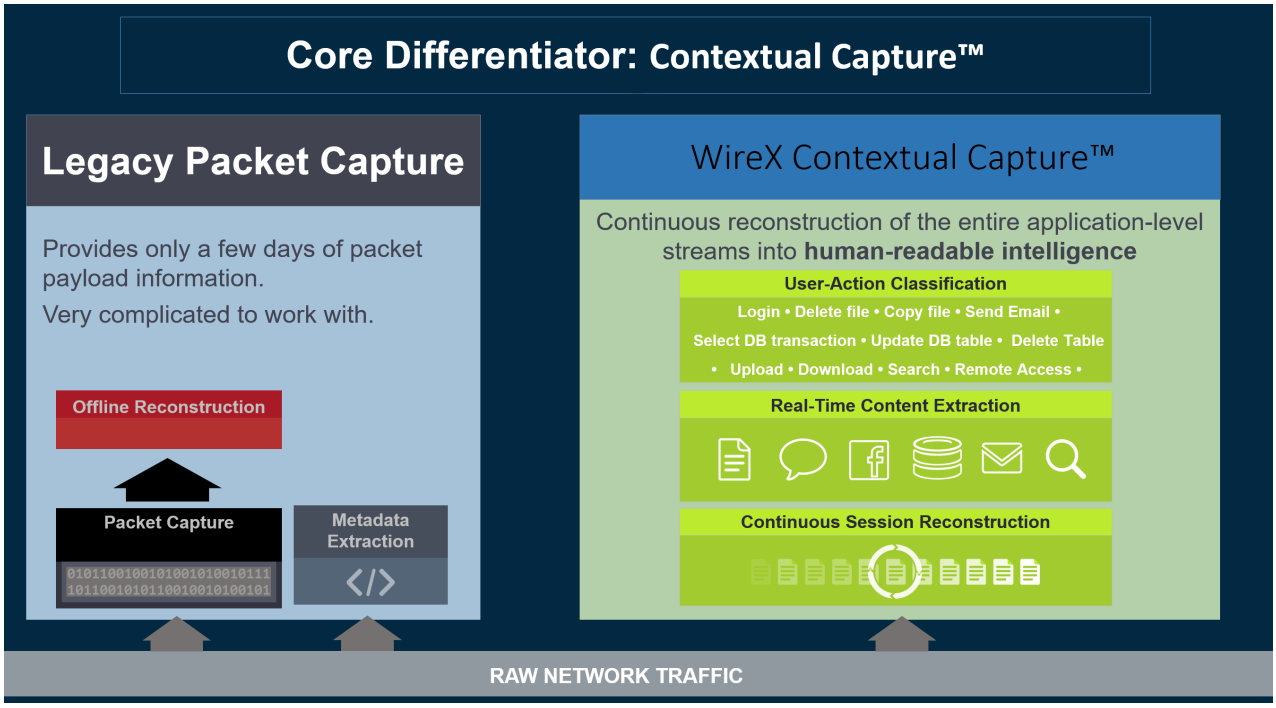
Distributed architecture designed to deliver true sustainable visibility into 100 Gbps networks:

- High performance database, optimized for large deployments
- Scalable capacity to store many months of complete intelligence
- Advanced filtering capabilities for analyzing 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
- Centralized management for a secure, single point of view, allowing multi-site and multi-sensor investigations

Security Investigation Framework

Steamline 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.
- Easy to use investigation and hunting interface, designed for all the different tiers within the team
- Built-in case management to support the entire investigation life-cycle
- Investigation playbook modeling capabilities and knowledge sharing across team members
- Open API- every insight can be easily exported to 3rd party tools



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.

For more information: www.wirexsystems.com