WireX Unique Selling Points

Despite the best efforts of security professionals and the proficiency of cyber security tools, security breaches constantly occur. Organizations are looking into network forensics solutions in order to be able to investigate the daily security alerts they are facing and to mitigate attacks in a timely manner.

WireX outperforms the existing forensics solutions in the market in the following aspects:

1. Delivers complete contextual understanding and visibility for security investigations

Requirement	Security teams need more context to mitigate security incidents. They need to be able to go back in time and understand what has happened. Spend millions on security tools, but can't handle all the different alerts triggered.
Problem	Existing solutions provide either too much or too little: • SIEM and other log-based solutions are only providing high level descriptions of what actually happened – not enough • Existing forensics tools are based on full packet capture and are overwhelming the team with data that is too slow to retrieve and too complicated to use. Furthermore, these solutions can handle mostly standard non-web protocols and in many cases they fail to provide context into more complex applications.
WireX Advantage	WireX introduces a unique analysis technology that extends enterprise visibility beyond metadata and overcomes the complexities and limitations with traditional packet-capture based solutions. • Security teams gain clear and immediate understanding of user behaviors and application contents across the enterprise network. • WireX's customizable analysis modules can provide the same level of visibility into proprietary business applications, as it do for enterprise applications • Due to its ability to scale, it can be deployed at the heart of the network and provide greater overall visibility, including DMZ and LAN

2. Faster time to resolution

Requirement	It takes too long to respond to incidents. Security teams need more effective investigation tools so that SOC could handle more alerts and escalate less. This also enables the escalation team to drill more quickly into what happened without wasting time on manual analysis.
Problem	Most organizations don't have the manpower to properly investigate every lead. With today's investigation tools security teams are still required to perform a lot of manual work in order to understand what has happened since the information is not easily accessible and understood.

WireX Systems Confidential & Proprietary. Copyright © 2020. All Rights Reserved

WireX Advantage	Adaptive, and easy to use investigation tool, allowing security professionals at all levels to handle security incidents quickly and effectively with the context they needs: • SOC is empowered with the ability to handle more complex investigations and can reduce the amount of escalations to higher tiers • IR / Escalation teams don't have to waste time collecting more intelligence to start an investigation

3. Removes skill-set barriers to supercharge forensics

Requirement	Enterprises need a solution that is easily usable and accessible across teams (analysts, SOC, escalation teams, etc.) each possessing a very different skill set.
Problem	Existing solutions require high-level expertise to be able to use the solution. Even at the well-funded, highly motivated companies are not able to translate it into real value, as the vast majority of the security team cannot operate the +1M$ solution.
WireX Advantage	WireX does all the heavy lifting of data analysis to remove skillset barriers. It delivers comprehensive security intelligence that can be immediately understood, regardless of security professional skill level. The solution can be used across the security organization (SOC, incident response, SIEM manager, etc.): • Intuitive query language enables powerful retrieval of relevant intelligence, without wasting precious time on manual examination of network sessions • It is integrated with the existing security infrastructure, to help streamline the investigation process and share knowledge across team members

4. Superior retention capacity and throughput to boost forensics history

Requirement	Enterprises need to collect network data for forensics for longer retention times (months to a year vs 10-30 days) and in high bandwidth segments (e.g. data center, LAN)
Problem	Existing solutions are based on full packet capture and therefore it's virtually impossible to scale (11TB to store a single day of 1Gbps network). 80% of the price for such deployments is for storage costs. Organizations are looking for a better alternative, or to complements the existing packet-based forensics
WireX Advantage	WireX Contextual Capture technology dramatically increases retention periods to an estimated of 25X more history on the same amount of storage in compare to traditional PCAP-based forensics. Rather than simply capturing packets, Contextual Capture continuously translates raw network traffic into comprehensive intelligence, with details on user behaviors and application contents. This eliminates the need to store raw packets and provides clear and immediate understanding to security incidents.

WireX Systems Confidential & Proprietary. Copyright © 2020. All Rights Reserved

5. Efficient implementation

Requirement	A solution that is easy to deploy in a large scale
Problem	Implementations of legacy solutions are complex and expensive. They often require a lot of customization and hardware to deploy. Typical required rack space can reach 50U!
WireX Advantage	Very flexible deployment options with a solution that can easily scale to fit the needs of the largest organizations: • Single day deployment • Saves around X10 in rack space! • Single appliance to monitor 100G with advanced filters to analyze traffic selectively

6. Save security costs

Requirement	Maximize ROI on the forensics investment
Problem	The cost and complexity involved in the adoption of forensics solutions are making them not cost-effective in most environments: - Storage costs due to the need to store packets in Petabytes scale, reach up to 80% of the total solution price! - Traditional solutions are very complicated to operate, which limits their usage across the different teams, specifically among 1st and 2nd SOC tiers. This creates a major bottleneck in facilitating forensics investigations - organizations are left without the ability to validate the constant alerts triggered by their own security measures.
WireX Advantage	WireX delivers the most cost-effective solution in the market: • Dramatically reduce storage costs: WireX unique approach (with Contextual Capture) eliminates the need to store raw packets, hence provides up to 25X more retention history on the same amount of storage, with even greater context and visibility • Maximizes value of existing security investment: WireX remove skillset barriers, Empowers the entire security team with the ability to quickly validate threats, handle more complex investigations and escalate fewer tickets • Mitigate damage: While every organization may expect a compromise, the key question is how fast the security team reacts. The longer it takes to respond, the greater the risk of irreversible damage. WireX accelerate incident response processes and therefore shrinks the scale of potential breaches

WireX Systems Confidential & Proprietary. Copyright © 2020. All Rights Reserved

EXTRA LINK