SentryWire Overview

SentryWire is the Next Generation Packet Capture Tool and Network Security Platform that is based on a unique capture and storage architecture which breaks the performance, scalability and expense barriers of existing frameworks. The system supports capture rates from 1Mbps to +1Tbps, while providing real-time filtering and allowing retention of network traffic for weeks, months and even years at price points that can be as little as 20% of the cost of other systems.

Imagine a Hadoop like architecture that is engineered to scale out compute and storage to provide the fastest search in the industry even in packet stores of 100PB’s. The SentryWire system has high-speed packet recording with real-time analytics, visualization, and BPF-syntax filters. The system detects intrusions, minimizes damage caused by breaches and enables complete packet level analysis of any incident.

SentryWire’s NetFlow Analyzer gives you the forensics you require, providing real-time visibility into network bandwidth performance, traffic patterns, and user/application bandwidth utilization.

The SentryWire Packet Capture Platform allows an extended timeline of traffic to be recorded and analyzed at commodity prices using new or existing analytics. Why is it important to have an extended timeline of packet traffic stored? Because we know on average it takes 146 days to detect certain state sponsored intruders in a network and without a high fidelity recording of the network traffic enterprises cannot make a definitive determination of when intruders got in, how they got in or exactly what data was ex-filtrated.
End Forklift Upgrades & Re-Buys

Imagine buying an IT solution once and upgrading it as needed, without losing a penny on your investment. Start small, SentryWire can grow with your enterprise. As your network throughput increases, simply add another capture node. If you want to increase the amount of network traffic you retain simply add a storage node. You get uninterrupted value from your investment without ever re-buying storage or compute that you already own. Simply add capacity and throughput.

SentryWire, Gain Visibility

On average it takes 146 days to detect a breach in your network. Most companies only store 4 days of packets on average, that leaves you with 142 days of no visibility into what was happening on your network during the breach. The SentryWire Packet Capture Tool and Network Security Platform will provide you with visibility into your network and not leave you in the dark when a breach has occurred.

Technology Partners

SentryWire partners with the leading security solution providers to extend the power of our packet capture platform. This ecosystem of partner technologies includes governance, risk compliance management platforms, intrusion detection systems, behavior based solutions, hardware and OS providers, other security & industry solutions.