SentryWire
PACKET CAPTURE PLATFORM

GNV Get Network Visibility
Powered By KEYSIGHT ixia anue

Joint Solution Brief

Uncover Breaches Faster and Reduce Data Loss with SentryWire and Keysight's Network Visibility Platform

The Challenge

A Data Breach lifecycle is on average 277 days between detection and containment breach[1]. Without an extended timeline or high-fidelity recording of traffic, it can be difficult to field a successful network detection and response to determine—with certainty—when threat actors gained initial access, how they moved once inside the perimeter, and what systems or data was impacted.

Integrated Solution

Together with Keysight's Network Visibility Platform, SentryWire delivers greater visibility into an enterprise's network traffic history—both on-prem and in the cloud.

Key Benefits

- Traffic flows from anywhere in the network, from both virtual or physical infrastructure, can be tapped by Keysight's Network Visibility Platform thenSentryWise can record, stor, and catalogue for fast search
- Accelerate processing throughput with Keysight Network Visibility platform with NetStack capabilities by effectively filtering and distributing relevant traffic from across the network to SentryWire
- SentryWire leverages the Keysight Network Visibility platform's NetStack capabilities for automatic traffic load balancing and aggregation functionality to reduce bottlenecking and port oversubscription
- Using Keysight Network Visibility platform's SecureStack for real-time SSL decryption functionality, SentryWire gains increased visibility and by more effectively compressing decrypted packets achieves a longer storage timeline

Introduction

On average, organizations capture one to four days' worth of packets. For optimal network detection and response, or to support compliance standards and government regulations, that's simply not enough!

Fortunately, SentryWire provides an affordable alternative that can amplify data capture. At a price point below that of typical traditional packet capture solutions, SentryWire enables organizations to retain traffic for months or even years. In fact, it can store, archive, index, and quickly search 100 percent of the network packet traffic, including traffic in the cloud.

Together with Keysight's Network Visibility Platform, the SentryWire solutions give enterprises broad visibility into their traffic and control over how that traffic is handled on an extremely granular level. In the event of a security incident, forensic analysts can review and investigate the traffic history to pinpoint an attacker's entry point, identify the malware used, and uncover what data was exfiltrated.

The Keysight and SentryWire Joint Solution

If firewalls were fences and intrusion detection systems were alarms, network packet capture would be the video surveillance that could round out a security package and help uncover an intrusion. In other words, companies can augment their security posture by integrating a solution that correlates the capture, retention, and analysis of IP network data packets with SentryWire.

Based on a unique capture and storage architecture, SentryWire is a robust Network Security Monitoring (NSM) platform with full packet capture that breaks down the performance, scalability, and expense barriers of existing Network Detection Response (NDR) frameworks. An affordable, TiVo-like digital network recorder for Big Data security analytics, the platform can easily integrate with existing open source, proprietary, or enterprise security solutions such as a SIEM or SOAR platform used by security analysts and detection engineering teams. As well as instrument to any forensics, visualization, or analytics package on the market.

What's more, the SentryWire system supports and provides real-time event alerting with Critical Asset, IOC, and IDS Alert correlation to help network and security teams reduce their alert fatigue by triaging more effectively. As well as lossless capture rates from 1Mb to 100Gb. Other features include:

- Fast Search—Reviews large data quantities quickly and efficiently
- Open Architecture—Uses any commercial, open source, or in-house tools

- Compression—Amplifies raw storage capacity of approximately 5x
- Federation—Scales implementation—from core systems to branch offices—with multiple form factors

Integrated with Keysight's Network Visibility Platform to raise security awareness, SentryWire makes capturing and storing traffic affordable for any size organization, any network bandwidth, or any data retention parameter.

Key Keysight Network Visibility Platform features that augment the value of SentryWire technology deployments include:

Filtering traffic to only send relevant traffic: Keysight's Network Visibility platform uses context-awareness and security intelligence to deliver de-duplicated highly relevant traffic to SentryWire to help ensure that they only analyze traffic that provides security value.

Easy access to traffic from physical and virtual networks: Keysight's Network Visibility platform provides complete data access, resilience, context-aware data processing, and security intelligence processing to ensure the right data gets to SentryWire.

To monitor east-west data center traffic, Keysight taps virtual traffic and incorporates it into Keysight's Network Visibility platform for delivery to SentryWire on the physical network. This ensures the combined monitoring and analysis of all traffic and eliminates blind spots.

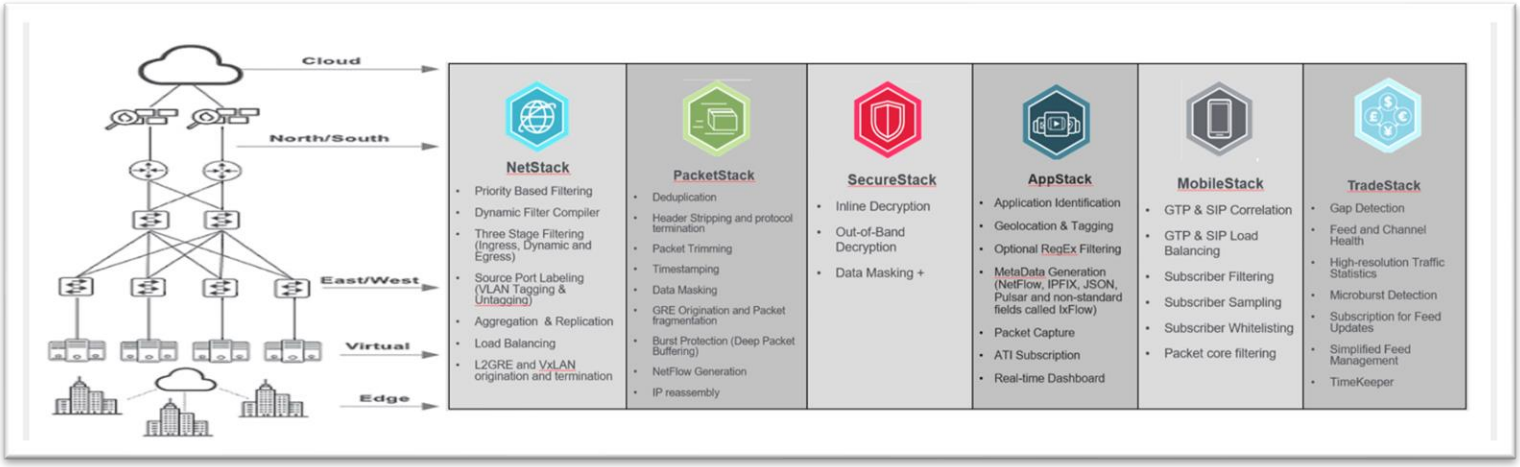
Together, the SentryWire and Keysight's Network Visibility platforms help organizations react faster to data breaches, reduce risk of data loss, and improve data protection practices to prevent unplanned outages.

Optimize tool processing throughput: Eliminate the need for tools to undertake complex and processor-demanding traffic transformations (e.g., SSL decryption) prior to processing. The Keysight Network Visibility platform uses context-awareness and security intelligence to deliver de-duplicated and highly relevant traffic SentryWire. Powered by dual data processing engines, SecureStack is the foundation for more robust inline security and faster out-of-band compliance and monitoring.

Easy access to traffic from physical and virtual networks: Keysight's Network Visibility platform provides complete data access, resilience, context-aware data processing, and security intelligence processing to ensure the right data gets to SentryWire.

To monitor east-west data center traffic, Keysight taps virtual traffic and incorporates it into Keysight's Network Visibility platform for delivery to SentryWire on the physical network. This ensures the combined monitoring and analysis of all traffic and eliminates blind spots.

Together, the SentryWire and Keysight's Network Visibility platforms help organizations react faster to data breaches, reduce risk of data loss, and improve data protection practices to prevent unplanned outages.



To learn more or for additional information on SentryWire and Keysight solutions, visit:

www.SentryWire.com
www.keysight.com

SentryWire
PACKET CAPTURE PLATFORM

GNV Get Network Visibility
Powered By KEYSIGHT ixia anue