Gigamon

SentryWire
PACKET CAPTURE PLATFORM

Joint Solution Brief

Uncover Breaches Faster and Reduce Data Loss with SentryWire and the Gigamon GigaSECURE Security Delivery Platform

The Challenge

On average, it takes 240 days to detect a network breach[1]. And without a high-fidelity recording of traffic, it's impossible to determine—with certainty—when cyber intruders got in, how they got in, and what they got away with.

Integrated Solution

Together with the Gigamon GigaSECURE® Security Delivery 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 Gigamon's Visibilty Fabric™ and recorded by SentryWire for utilization by any analysis tools available on the network
- Accelerate processing throughput with the GigaSECURE Security Delivery Platform by effectively filtering and distributing relevant traffic from across the network to SentryWire
- SentryWire leverages the GigaSECURE platform's automatic traffic load balancing and aggregation functionality to reduce bottlenecking and port oversubscription
- Using GigaSECURE's real-time SSL decryption functionality, SentryWire gains increased visibility into traffic without network performance degradation

Introduction

On average, companies capture four days' worth of packets. For optimal data security and analysis, 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 filter 100 percent of traffic, including traffic between virtual machines in the cloud.

Together with the GigaSECURE Security Delivery 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 in order to pinpoint an attacker's entry point, identify the malware used, and uncover what data was exfiltrated.

The Gigamon and SentryWire Joint Solution

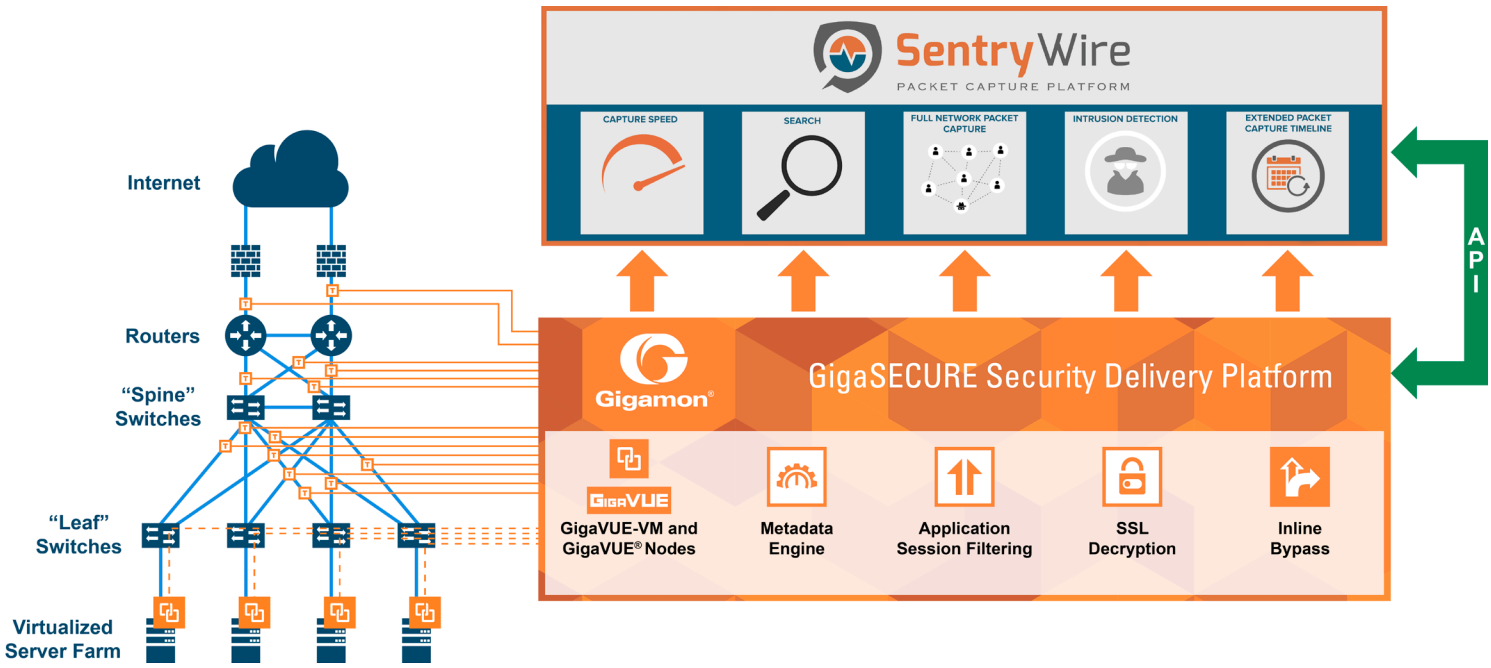
If firewalls were fences and intrusion detection systems were alarms, network packet capture would be the video surveillance that could round out a security package and help uncover an intrusion. In other words, companies can augment their security posture by integrating a solution that correlates the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

Based on a unique capture and storage architecture, SentryWire is a next-gen network packet capture platform that breaks down the performance, scalability, and expense barriers of existing frameworks. An affordable, TiVo-like digital network recorder for Big Data security analytics, the platform can integrate with open source or proprietary security solutions like IPS and IDS 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 filtering for known signatures 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 custom cyber tools

[1]Source: www.sentrywire.com



- Compression/Compaction—Amplifies raw storage capacity by 5-30x
- Federation—Scales implementation—from core systems to branch offices—with multiple form factors

Integrated with the Gigamon GigaSECURE Security Delivery Platform and to raise security awareness, SentryWire makes capturing and storing traffic affordable for any size organization, any network bandwidth, or any data retention parameter.

Key GigaSECURE Security Delivery Platform features that augment the value of SentryWire technology deployments include:

Filtering traffic to only send relevant traffic: The GigaSECURE platform can be configured to send only relevant traffic or sessions to the SentryWire and Sentry Cloud solutions to help ensure that they only analyze traffic that provides security value.

Optimize tool processing throughput: Eliminate the need for tools to undertake complex and processor-demanding traffic transformations (e.g., SSL decryption) prior to processing. With the GigaSECURE Security Delivery Platform, SentryWire can concentrate on processing traffic rather than converting it into the right format.

Easy access to traffic from physical and virtual networks: The GigaSECURE platform manages and delivers network traffic—in the correct format—to SentryWire. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the GigaSECURE 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 Gigamon platforms help organizations react faster to data breaches, reduce risk of data loss, and improve data protection practices to prevent unplanned outages.

Learn More

For more information on SentryWire and Gigamon solutions, contact:

SentryWire
PACKET CAPTURE PLATFORM
www.SentryWire.com

Gigamon®
www.gigamon.com

3203-01 08/16