Solution Brief

# Tenable and Gigamon

## Continuously Monitor Encrypted Traffic to Identify Risk

## Key Challenges

In order to fully secure your network, you must have a good understanding of what's in it and what's at risk. A good way to identify connecting devices and their vulnerabilities is to periodically perform active vulnerability scanning and passively monitor network traffic between active scans to detect new devices and identify new risks.

However, passive monitoring is difficult when traffic being inspected is encrypted. Without the ability to decrypt and analyze this traffic, organizations may be unable to fully understanding their exposure and risk. In addition, span ports on network switches are precious, so deployments that provide traffic mirroring and forwarding for analysis by multiple tools are preferred.

A solution that supports active scanning and non-intrusive passive monitoring along with the ability to look inside encrypted traffic can help continuously monitor your environment for vulnerabilities, threats and misconfigurations.

## Solution Overview

Gigamon's GigaVUE-H Series nodes offer the ability to decrypt SSL or TLS traffic providing advanced visibility for enterprises, federal organizations and service provider infrastructure. Organizations can maximize span port usage with Gigamon GigaVUE, enabling multiple tools to receive decrypted traffic for analysis.

Tenable Nessus® Network Monitor accepts decrypted traffic from Gigamon and inspects network traffic to identify new or unmanaged devices connecting to your environment and associated vulnerabilities. It also non-intrusively identifies relevant context from the traffic stream to identify OS information and application identification for forensics analysis and threat identification.

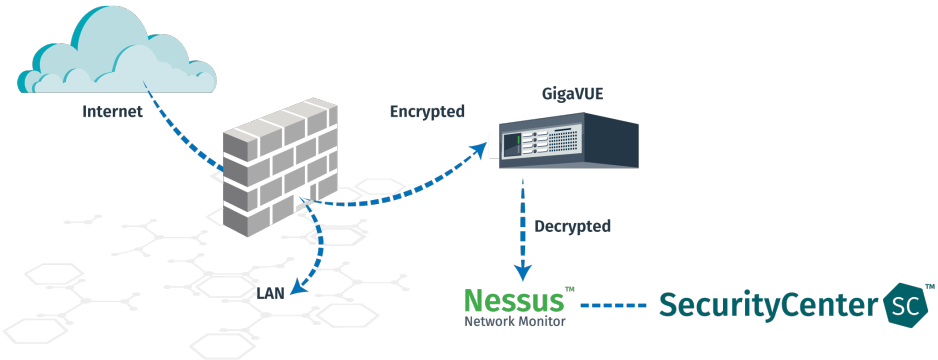
When Nessus Network Monitor is deployed as part of SecurityCenter Continuous View® (SecurityCenter CV™), customers receive the added benefit of Tenable Nessus active scanning and log analysis along with continuous network traffic monitoring. The integration with Gigamon enables you to have a complete view of managed and unmanaged devices connecting to the network and the risk they pose even when traffic is encrypted.

### Components:

- Tenable Nessus Network Monitor 4.x
- Tenable SecurityCenter CV 5.x
- Gigamon GigaVUE-HD, -HC and -HB products

### Benefits:

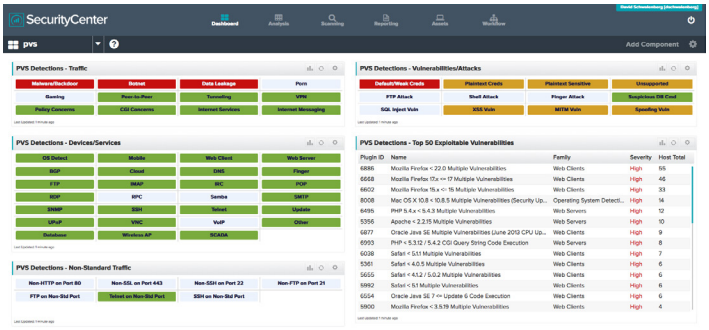
- Provides continuous visibility into network devices and applications that introduce risk
- Eliminates blind spots on your network caused by encryption
- Improves the accuracy of vulnerability assessments by detecting vulnerabilities between scans
- Reduces risk by better identifying and non-intrusively monitoring encrypted traffic



Tenable™ offers two solutions that provide integration with Gigamon.

**Nessus Network Monitor:** A standalone traffic monitoring solution that non-intrusively identifies devices, applications and vulnerabilities on your network.

**SecurityCenter Continuous View:** A continuous monitoring solution that provides complete visibility of your environment, including the deepest detection of vulnerabilities, misconfigurations, malware and real-time threats, the most advanced analytics, and the industry's only Assurance Report Cards®. Architected to include multiple technologies, including traffic monitoring, SecurityCenter benefits from the visibility provided by GigaVUE's traffic decryption capabilities for continuously analyzing encrypted traffic for vulnerabilities and risk.




*When GigaVUE decrypts encrypted traffic and forwards it to Tenable SecurityCenter CV, customers gain improved visibility into potential risks including vulnerabilities identified from inspecting encrypted traffic.*

## How It Works

**Step 1.** Install your Tenable solution according to the instructions in its User Guide. Then install the GigaVUE appliance per the installation guidelines provided by Gigamon.

**Step 2.** Configure your Gigamon appliance to decrypt SSL or TLS encrypted traffic. GigaVUE will aggregate, process and filter the network traffic.

**Step 3.** Configure your Gigamon appliance to forward the decrypted traffic either to your Nessus Network Monitor or SecurityCenter CV for vulnerability and risk analysis.

**Step 4.** Verify that your Tenable solutions can see the traffic from Gigamon as well as all other network traffic for vulnerability and risk assessment.

## Benefits

By deploying Gigamon and Tenable solutions together, organizations that have encrypted traffic in their environments can regain visibility into what devices are connecting to their environment and continuously monitor network traffic to identify vulnerabilities and risk.

## About Gigamon

Gigamon provides an intelligent Visibility Fabric™ architecture for enterprises, data centers and service providers around the globe. Our technology empowers infrastructure architects, managers and operators with pervasive and dynamic intelligent visibility of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies and centralized management, the Gigamon GigaVUE® portfolio of high availability and high-density products intelligently delivers the appropriate network traffic to management, analysis, compliance and security tools. With over eight years' experience designing and building traffic visibility products in the US, Gigamon solutions are deployed globally across vertical markets including over half of the Fortune 100 and many government and federal agencies. - See more at: gigamon.com.

## About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

tenable™

**For More Information:** Please visit tenable.com
**Contact Us:** Please email us at sales@tenable.com or visit tenable.com/contact