Joint Solution Brief

Detect Assets, Vulnerabilities and Threats in Your Infrastructure

The Challenge

As the size and complexity of a network grows, so does the challenge of ensuring you're not making it easy for attackers to access and control sensitive data. Monitoring for vulnerabilities such as misconfigurations, use of default passwords and missing patches is an essential function for the Security Operations Center.

Integrated Solution

Tenable is the market-leading network vulnerability scanning solution deployed to detect vulnerabilities that can be exploited to compromise network cybersecurity. Gigamon helps ensure your Tenable deployment has efficient access to any traffic traversing your network – whether it is from a physical, virtual, or public cloud infrastructure—even if it is SSL/TLS encrypted.

Joint Solution Benefits

- Provides continuous active and passive scanning for the detection of exploitable vulnerabilities on the network
- Provides both agentless and agent-based scanning options
- Protects the IT environment by running vulnerability scans, configuration and compliance checks, malware detection, web application scanning and more
- Visibility into network traffic whether encrypted or not
- Maximise architectural and operational efficiency: aggregate traffic to centralized 10Gb devices; intelligent load balancing across multiple appliances and intelligent filtering minimize unnecessary traffic analysis and processing
- Gigamon provides an excellent source of unsampled metadata (Netflow or IPFIX) for Tenable analysis through Tenable NetFlow Monitor

Introduction

Complex, distributed, and virtualized networks present a large surface area of attack to cyber adversaries. IT systems have often been built to server-specific functions and communicate with other systems without taking cybersecurity as a primary consideration. The use of new technologies such as public cloud or virtualization, coupled with user activity create additional opportunities for vulnerabilities.

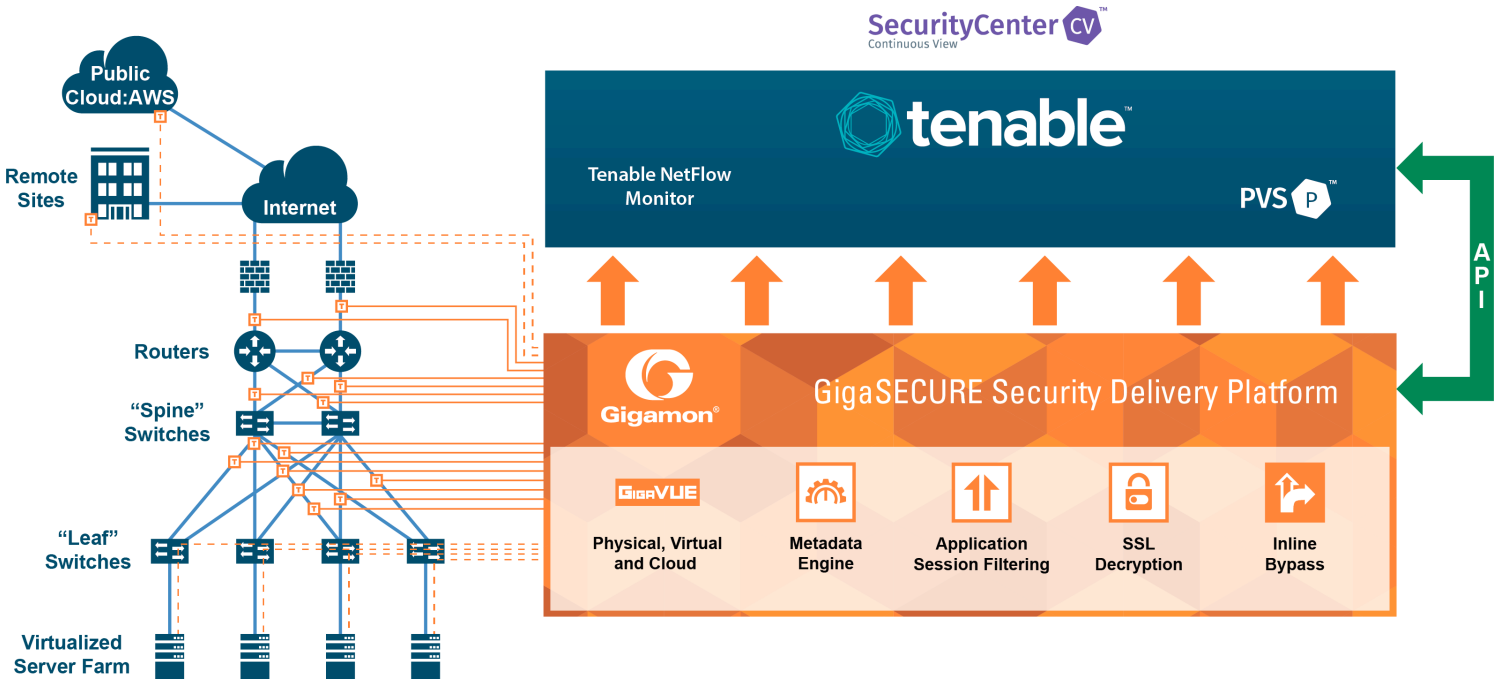
Securing these environments requires a combination of active scanning for detection of systems-based vulnerabilities and passive scanning for vulnerabilities present in data in motion. Vulnerabilities need to be identified and corrected to avoid presenting bad actors with opportunities to access and exploit valuable organizational information or to disrupt operational business.

Any solution has to provide a combination of the analytics required together with a pervasive and efficient reach across the network infrastructure, ensuring complete coverage and protection. That includes being able to analyze the growing volume of encrypted traffic flowing across the network.

The Gigamon and Tenable Joint Solution

Gigamon and Tenable deliver a joint solution that optimizes network cybersecurity vulnerability detection and remediation. Tenable uses agent-based and agentless active scanning to secure the IT environment by running vulnerability scans, configuration and compliance checks, malware detection, web application scanning, and more. Passive scanning through the Tenable PVS component exposes vulnerabilities hidden in data in motion. Tenable Security Center provides centralized visibility into detected vulnerabilities in need of remediation.

The scale and technical complexity of modern networks all present a challenge to effective passive scanning, but the Gigamon solution works with Tenable to help solve these challenges. The Gigamon Visibility Platform provides IP packet-level visibility across complex, distributed and virtualized networks (including public cloud). It aggregates data for monitoring, decrypts SSL/TLS packets and applies intelligent processing in real-time to create custom data sets for the Tenable PVS servers. If Netflow or IPFIX records are required, the Gigamon platform can generate these from any monitored traffic flow and deliver them to the Tenable Netflow Monitor for processing and analysis.



Through advanced filtering and other techniques, PVS server effectiveness can be optimized; data is available from across the entire enterprise, but only relevant data needed for vulnerability detection needs to be processed. Gigamon allows for the consolidation and centralization of the PVS servers, enabling deployment of 10Gb PVS servers in an array with load balancing and failover. De-duplication and advanced filtering techniques helps ensure PVS servers only need to process relevant traffic. Consolidating a distributed PVS deployment to a centralized solution can significantly reduce the CAPEX and OPEX needed for effective network coverage, while improving reliability and availability of the passive scanning function.

Learn More

For more information on the Tenable and Gigamon solution, contact:

tenable
www.tenable.com

Gigamon®
www.gigamon.com

3222-01 03/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com