Gigamon ThreatINSIGHT™ Sensor Overview

Gigamon ThreatINSIGHT sensors are one critical component to accessing the ThreatINSIGHT network capabilities. Each sensor needs to be strategically placed within the customer infrastructure, so it has visibility into network traffic needed to meet a customer's security objectives. Given the diverse nature of network architectures, infrastructure, and monitoring needs there is no one-size-fits-all solution. To meet the needs of its customers, Gigamon offers several types of sensors that can be deployed into almost any network environment.

Sensor Types	Specifications	Sustained Throughput	On-Prem	Cloud Platform
Gen 3 GigaVUE-HC1	GigaSMART Cards (V5.10.01)	2 Gbps / engine 4 Gbps / chassis	✓	
Large Appliance	1U with 2x Copper / 2x Fiber[1]	10 Gbps	✓	
Small Appliance	1U with 2x Copper / 2x Fiber[1]	2 Gbps	✓	
Virtual ESXi Sensor	Minimum 4 Cores / 8GB RAM	0.9 - 5 Gbps*	✓	✓
Virtual KVM Hypervisor Sensor	Minimum 4 Cores / 8GB RAM	0.9 - 5 Gbps*	✓	✓
Azure Virtual Image	Minimum D4d v4 Instance	0.8 - 3.2 Gbps*		✓
Amazon EC2 Machine Image	Minimum m5.xlarge Instance	0.7 - 3.2 Gbps*		✓

[1] Any combination of 2 ports may be active for ingestion

*Maximum sustained throughput is achieved with increased Cores/RAM or larger instances

Network Requirements

ThreatINSIGHT sensors are designed to run off a SPAN port, TAP interface, or receive network traffic from a packet broker. Sensors are placed strategically throughout the network based on the customer's goals. Placement often includes visibility to North/South traffic and major East/West links (especially around critical infrastructure) and to cloud or IaaS (Infrastructure as a Service) environments that often go completely unmonitored. Each sensor is pre-configured by Gigamon and all that is required beforehand is an IP, subnet mask, and gateway. Each customer will work with the INSIGHT team to ensure the sensor is receiving appropriate data. Large and small sensors come with multiple monitoring ports to keep the footprint within the data center to a minimum.

Sensor Visibility Points

DEPLOYMENT OPTIONS FOR COVERAGE

Gigamon ThreatINSIGHT provides unequaled visibility across your attack surface (N/S/E/W + AWS/Azure/Cloud + remote sites) enabling high-fidelity, ML & behavior-based threat detection and rapid, informed response through threat hunting and complete incident investigations.

A More Powerful Security Stack

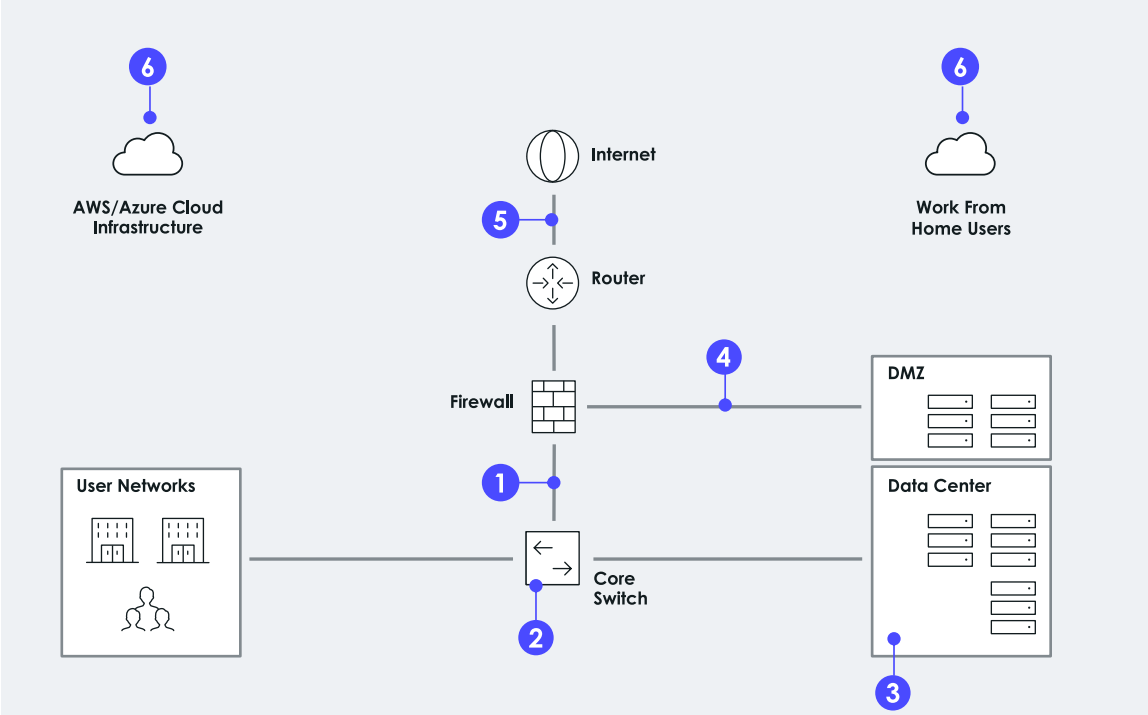
Gigamon®

Visibility & Analytics Fabric

+

GigaSMART

ThreatINSIGHT is easily enabled or deployed with Gigamon Visibility and Analytics Fabric™ and GigaSMART®



1. EGRESS POINTS

+ Captures north/south traffic from clients and servers
+ Enables detection of exfiltration, C2, tunneling, beaconing

2. CORE SWITCH

+ Captures east/west traffic between clients and servers
+ Enables detection of lateral movement, staging, internal threats

3. DATA CENTER

+ Captures east/west traffic between servers (including virtual)
+ Enables detection of data theft, unauthorized access

4. DMZ

+ Captures north/south traffic between DMZ and external clients
+ Enables detection of unauthorized access, vulnerability exploitation, exfiltration

5. EXTERNAL LINK

+ Captures north/south traffic between external clients and the internal networks. Provides visibility to traffic even if it is blocked by the firewall
+ Enables detection of exploitation attempts

6. CLOUD VISIBILITY

+ Cloud infrastructure workload traffic analysis via AWS/Azure Machine Images or VM/KVM
+ Work from home via 3rd party integrations (e.g. Zscaler)
+ Enables detection of un-managed and IoT devices

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

01/2020