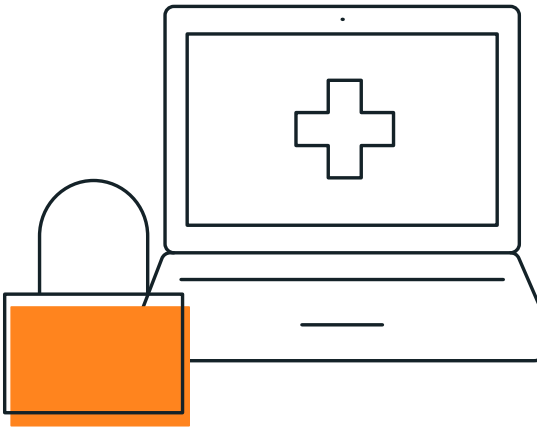
Gigamon® | MEDIGATE

Secure IoT Healthcare Devices — and Your Network — With Gigamon and Medigate



THE CHALLENGE

Connected devices are revolutionizing healthcare and making it harder to secure the network. As IT, operational technology, internet of things (IoT) and cyber-physical systems (CPS) converge, bad actors are exploiting vulnerabilities across new and old infrastructure. To combat the issue, healthcare organizations must find a solution that ensures the usability of all connected devices without compromising security.

THE SOLUTION

Working together, the Gigamon Visibility and Analytics Fabric™ (VAF) and Medigate Device Security Platform (MDSP) provide healthcare organizations with the ability to see, secure and manage their connected devices, while turning their data into a powerful analytics resource.

JOINT SOLUTION BENEFITS

+ Mitigate security risks associated with a rise in IoT devices
+ Identify anomalous behavior, communications and traffic behaviors quickly
+ Strengthen your overall security posture and keep medical care devices and operations safe
+ Prevent overload by sending only relevant traffic to connected tools
+ Extend the useful life of your monitoring infrastructure and safely delay costly upgrades

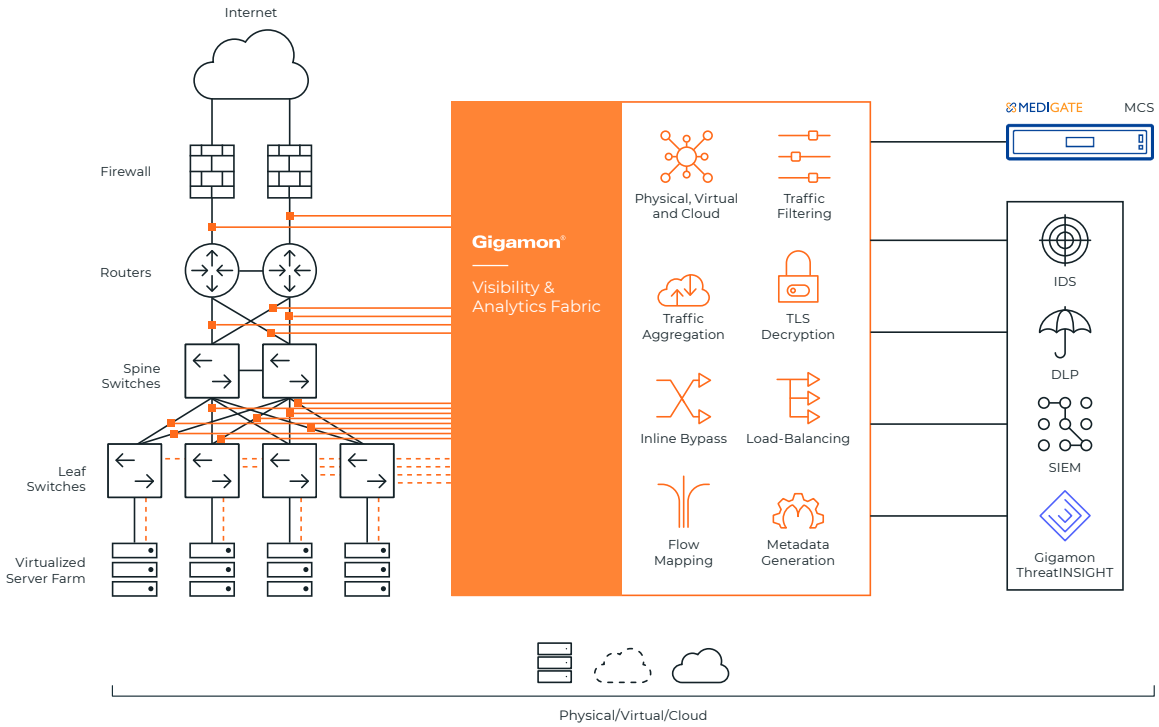
Introduction

The Medigate Device Security Platform (MDSP) continuously discovers and evaluates every connected device in a healthcare environment and provides real-time, detailed device inventory and evaluation of risk. Leveraging MDSP's contextual understanding of device function, the platform can recommend pre-defined, clinically vetted enforcement policies, helping to ensure that the facility can contain and mitigate threats.

The Gigamon + MDSP Joint Solution

Key Gigamon VAF features that enhance the value of MDSP to protect against network threats include:

+ **Easy access to traffic from physical and virtual networks:** The Gigamon VAF manages and delivers all network traffic — including East-West datacenter traffic and private and public cloud workloads — to the MDSP tool so all traffic can be monitored and analyzed together, reducing blind spots and increasing the likelihood of spotting suspicious behavior.
+ **Aggregation:** The Gigamon VAF selectively aggregates all traffic to be monitored and analyzed together, reducing blind spots and increasing the likelihood of spotting suspicious behavior and covering the issue of asymmetric routing and link aggregation groups. By tagging the traffic, the Fabric ensures the source of traffic can be identified.
+ **Traffic filtering:** The VAF can be configured to only send relevant traffic — or relevant sessions — to MDSP ensuring it doesn't become overloaded with irrelevant traffic.
+ **Load balancing to spread traffic across multiple devices:** When traffic flows are too large for a single MDSP instance, the VAF can split the flows across MDSP instances, while ensuring sessions are kept together. Additionally, the number of MDSP instances can be incrementally grown by adding new instances.



+ **Metadata (NetFlow/IPFIX) generation to be consumed by tool:** Gigamon devices can generate unsampled NetFlow/IPFIX metadata for any traffic flow. Gigamon also generates extended metadata records for things like HTTP response codes and DNS queries. This extended metadata can be used to provide far more detailed contextual analysis when looking at network and security events.
+ **Resilience of solution:** Deploy security devices inline and use the Gigamon Inline Bypass functionality to provide physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure.
+ **SSL decryption:** The VAF decrypts SSL/TLS encrypted traffic (including TLS 1.3) for inspection by MDSP and any other monitoring devices.
+ **Header stripping for efficiency:** If the MDSP doesn't analyze or understand certain encapsulation or tagging headers within a packet, the VAF can remove these headers before sending the packet to the tool for processing. This increases MDSP's effectiveness and efficiency.
+ **Packet or flow slicing for efficiency:** If the connected tool doesn't need to see the body information within the packet, the VAF can remove it before sending the packet headers to the tool for processing. This reduces load on the device and increases its efficiency.
+ **Masking for security/compliance:** The VAF can mask private, sensitive or confidential data within packets before they're sent to MDSP, where they may be seen by unauthorized people.
+ **Deduplication:** Pervasive visibility requires tapping or mirroring traffic from multiple points in the network, which in turn, means tools may see the same packet more than once. To avoid the unnecessary packet-processing overhead on the MDSP tool, the VAF removes duplicates before they consume resources.

For more information on Gigamon and Mediate, visit: www.gigamon.com and www.medigate.io.

© 2021 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Gigamon®

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