JOINT SOLUTION BRIEF

Gigamon and Pulse Enable Secure Access from Any Device

The Challenge

BYOD and the merging of OT and IT are driving a proliferation of connected devices — many of which aren't secure — creating a much larger attack surface for you to defend. If you don't have pervasive visibility across all these devices, you won't detect threats quickly enough to act before the damage is done.

Integrated Solution

Pulse Policy Secure provides easy, comprehensive secure access solutions for people, devices, things and services. Gigamon sends consolidated traffic information with dynamic filtering to Pulse Policy Secure, providing users with full visibility across all devices, greater efficiency and automated endpoint security compliance. Pulse Policy Secure also leverages the endpoint contextual information received from Gigamon for User and Entity Behavioral Analytics (UEBA) to detect IoT anomalies, DGA attacks, MAC spoofing, and provide Adaptive Authentication to avoid unauthorized access to the network.

Joint Solution Benefits

- Support Zero Trust strategies. Discover, profile and securely connect users and devices according to policy.
- Define security posture policies for user roles and endpoints. Then automatically enforce them on all endpoints (based on identity, role or device class) before they are allowed on the network.
- Improve overall security. Dynamic network segmentation at the network edge prevents threats from spreading laterally, and bidirectional integration with the security infrastructure (SIEM and NGFW, for example) enables fast threat response at the endpoint level.
- 360 degree endpoint insight. Pulse Policy Secure continuously monitors for suspicious state changes and provides reports about endpoint trends.
- Behavioral Analytics. Correlation of user access, device contextual information, system logs in a new analytics engine to find out anomalies and mitigate threat risk.

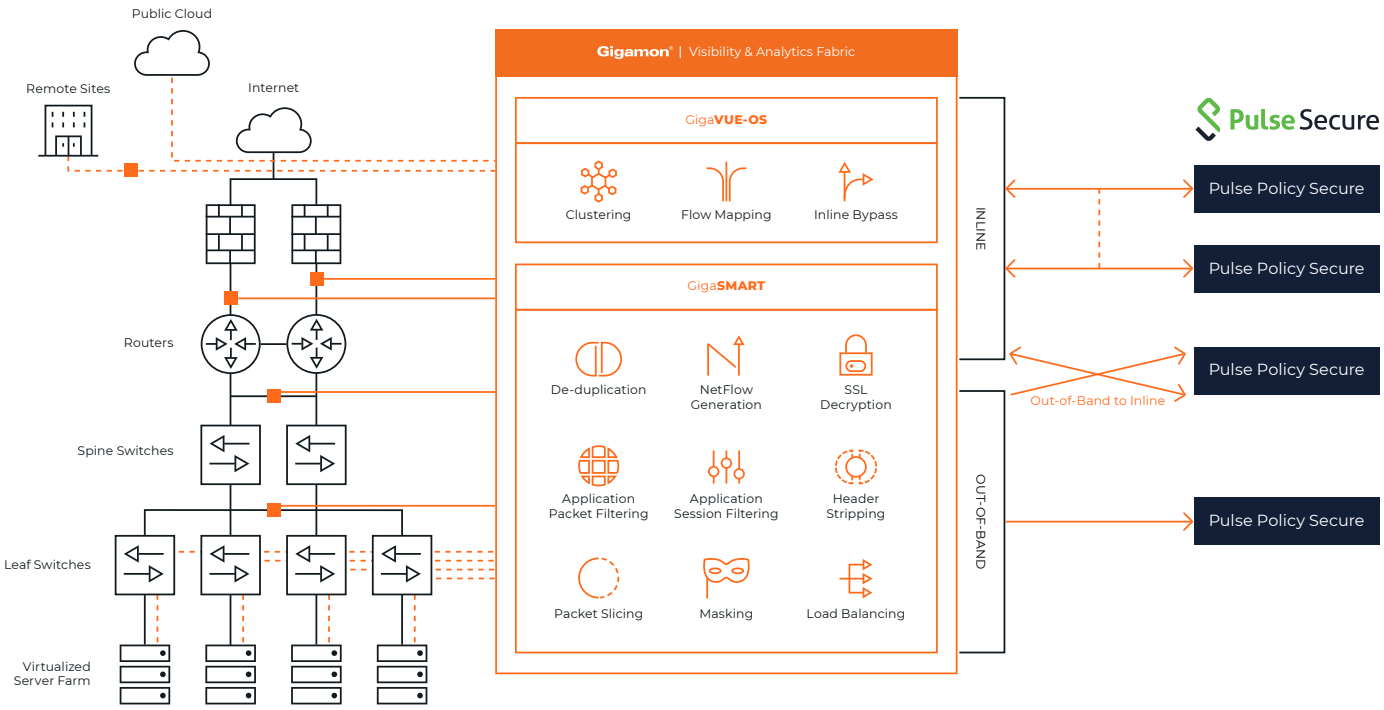
Introduction

With Pulse Policy Secure and Gigamon, empower your mobile workforce to securely access applications and information in the data center and cloud, while ensuring endpoint security compliance.

The Gigamon–Pulse Secure Joint Solution

Key Gigamon Visibility and Analytics Fabric™ features that enhance Pulse Policy Secure include:

- **Easy access to traffic from physical and virtual networks:** The Gigamon Visibility and Analytics Fabric manages and delivers all network traffic — including east-west data center traffic and private and public cloud workloads — to tools so all traffic can be monitored and analyzed together, reducing blind spots and increasing the likelihood of spotting suspicious behavior.
- **Metadata (NetFlow/IPFIX) generation:** Gigamon nodes 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.
- **Traffic filtering:** The Gigamon Visibility and Analytics Fabric can be configured to send relevant traffic — or relevant sessions — to the connected tools, so Pulse Policy Secure doesn't become overloaded with irrelevant traffic.
- **Aggregation to minimize port tool use:** Where links have low traffic volumes, the Gigamon Visibility and Analytics Fabric can aggregate these together before sending them to the Pulse Policy Secure tool in order to minimize the number of ports that need to be used. By tagging the traffic, the Fabric ensures the source of traffic can be identified.
- **Easier control of asymmetric routing to help ensure session information is kept together:** Most security devices require that all the packets in a session be inspected by the same device since incomplete sessions risk being blocked. The Gigamon Visibility and Analytics Fabric provides an intelligent and efficient way to help ensure this inspection happens in most architectures.
- **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.
- **Deduplication:** Pervasive visibility requires tapping or copying 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 Pulse Policy Secure, the Gigamon Visibility and Analytics Fabric removes duplicates before they consume resources.



For more information on Gigamon and Pulse Secure, visit gigamon.com and pulsesecure.net

Gigamon®

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