Pulse Secure And Gigamon Announce Network Security Solution For Real-Time Visibility Of Network-connected Devices

Published on 26 Jun 2020

Pulse Secure, the provider of software-defined Secure Access solutions, announced successful integration and joint compatibility testing between Gigamon and Pulse Secure to ensure customers that Pulse Secure’s Network Access Control (NAC) solution, Pulse Policy Secure, can fully leverage the endpoint contextual information received from Gigamon as remote workers return back to their office.
The combination of Gigamon and Pulse provides organizations real-time visibility of network-connected devices and Zero Trust control leveraging adaptive authentication and User and Entity Behavior Analytics (UEBA) to detect anomalies and mitigate unauthorized and malicious access to network applications and resources.

**Traffic information with dynamic filtering**

Pulse Policy Secure is a full-featured Network Access Control solution that is easy to deploy, manage, integrate and scale. Gigamon, sends consolidated traffic information with dynamic filtering to Pulse Policy Secure to enhance endpoint visibility across distributed networks and more automated endpoint security compliance.

Ensure that critical security analytic data flows seamlessly across solutions to provide the visibility and control.”

Leveraging Pule Secure UEBA features, Pulse Policy Secure can identify and respond to anomalous activity such as suspicious IoT activity, DGA attacks and MAC spoofing as part of the solution’s adaptive authentication capabilities aligning to Zero Trust control.

“The growing adoption of Zero Trust makes it essential that the security vendor community works in concert to ensure that critical security analytic data flows seamlessly across solutions to provide the visibility and control enterprises need to make better informed secure access decision in real time,” said Alex Thurber, Chief Revenue Officer for Pulse Secure. “We have worked closely with Gigamon at a technical level to create a smooth integration process with capabilities that will ensure our joint customers gain tangible benefits in deploying our technologies together to aid both network management and secure access in support of Zero Trust.”

**Granting network access according to security posture**
Joint Solution Benefits include:

- Support Zero Trust strategies. Discover, profile and authenticate users and devices prior to granting access according to their security posture.

- Define security posture policies for user roles and endpoints. Then automatically enforce access rules on all endpoints (based on identity, role, device class and security posture) before they are allowed on the network.

- Improve overall security. Enforce dynamic network segmentation of devices at the network edge to prevent threats from spreading laterally, and enable bidirectional integration with the security infrastructure (SIEM and NGFW, for example) for expedited threat response.

- 360-degree endpoint insight. Pulse Policy Secure captures in-depth endpoint intelligence and continuously monitors for suspicious state changes to provide reports about access issues and trends.

- Behavioral Analytics. Correlation of user access, device contextual information, and system logs in a new analytics engine to find anomalies and mitigate threat risks.

**Monitoring all network traffic for suspicious behavior**

Pulse Policy Secure captures in-depth endpoint intelligence and continuously monitors for suspicious changes.

Pulse Policy Secure integrates with the Gigamon Visibility and Analytics Fabric, which is used to monitor all network traffic - including east-west data center traffic and private and public cloud workloads - so all traffic can be analyzed together in order to reduce blind spots and increase the likelihood of spotting suspicious behavior.

“Ecosystem partnerships are essential to the adoption of Zero Trust initiatives and working closely with key Secure Access vendors, such as Pulse Secure, to help ensure seamless integration is vital for customers to maximize their return on investment”
,” said Gigamon President and Chief Operating Officer Shane Buckley. “As organizations strive to do more with fewer resources, they often turn to automation to help realize benefits that are greater than the sum of their contributing parts.”

Additional benefits of using Gigamon alongside Pulse Secure include traffic aggregation to minimize port utilization. In cases where network links have low traffic volumes, the Gigamon Visibility and Analytics Fabric can aggregate these together before sending them to the Pulse Policy Secure NAC solution 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 easily identified.

“Where network links have low traffic volumes, the Gigamon Visibility and Analytics Fabric can aggregate these together”

**Endpoint information and fortified security analytics**

In addition, Gigamon Visibility and Analytics Fabric offers enhanced control of asymmetric routing to ensure session information is kept together. Pulse Policy Secure gains the complete context of an endpoint’s connections and fortified security analytics.

“Based on the principle of ‘never trust, always verify,’ Zero Trust Networking (ZTN) requires the coordination of various security technologies to enable perimeter enforcement, network segmentation and adaptive access control,” said Tony Massimini, senior industry analyst at Frost & Sullivan. “Vendor collaboration, such as that between Gigamon and Pulse Secure, demonstrates the value of interoperability that supports customers advancing Zero Trust initiatives.”

The enhanced integration capability is freely available as part of the standard licensing model for both platforms, as part of Pulse Policy Secure and Gigamon Visibility and Analytics Fabric. Pulse Secure Partners also offers Gigamon solutions to its client base, making the partnership of particular relevance to the security channel community.
The Growth Of The Mobile Access Card Market In 2020

The emergence of smartphones using iOS and Android is rapidly changing the landscape of the IT industry around the world. Several industries...

The Digital Transformation Of Modern Access Control Solutions

The safeguarding of premises through the monitoring of entrance and exit points has traditionally been a very manual aspect of security. Hum...

The Increased Role Of Video Surveillance Technology In Our Changing En...

Today’s environment has evolved into something that according to some may seem unexplainable. But in the context of video surveillance...