Joint Solution Brief

Gigamon and ForeScout – Smart Usage of Network Traffic

The Challenge

A huge variety of devices are joining your network daily. These devices significantly expand your attack surface, yet are invisible to many security products because they are often misidentified. Historically, active scanning has been used to identify these devices but 100 percent passive discovery and continuous visibility is now the requirement for securing business networks without any impact to business operations.

Integrated Solution

The ForeScout solution integrates with the customers' IT environments for the purpose of providing visibility and control for all network connected devices. One very significant source of information is network traffic. The Gigamon GigaSECURE® Security Delivery Platform helps maximize the ability for ForeScout to leverage network traffic by helping to ensure it has easy and efficient access across the network without introducing any 'in-line' failure risk.

Joint Solution Benefits

- Consolidated traffic information for ForeScout to leverage in discovery, classification and compliance monitoring policies from a centralized location.
- Collection of traffic from 'air-gapped' networks to be provided 'out-of-band' to ForeScout, allowing visibility without impacting the air-gap.
- Flexible scalability, matching network speeds, traffic relevance and throughput requirements to help ensure solution efficiency.
- Dynamic filtering of irrelevant traffic for increased ForeScout efficiency.
- Optional decryption features help ensure any information within packet data can be analyzed and used for end point classification.

Introduction

A foundational element of network security is knowing what is on the network and how each infrastructure device is behaving. New devices such as unmanaged laptops, smartphones, tablets, Internet of Things (IoT) devices of all shapes and sizes, rogue devices, virtual servers and public cloud instances join your network nearly every hour. Bring Your Own Device (BYOD), IoT and datacenter (DC) security all rely heavily on segmentation as an information security best practice. While a very good practice, segmentation introduces its own set of issues, particularly for network traffic visibility. In addition to segmentation contraints, operational technology (OT) environments are often air-gapped, creating their own set of traffic visibility challenges. Customers are looking for a flexible solution that allows distributed traffic capture, consolidation and centralized delivery to an analysis technology in order to maximize coverage and capabilities.

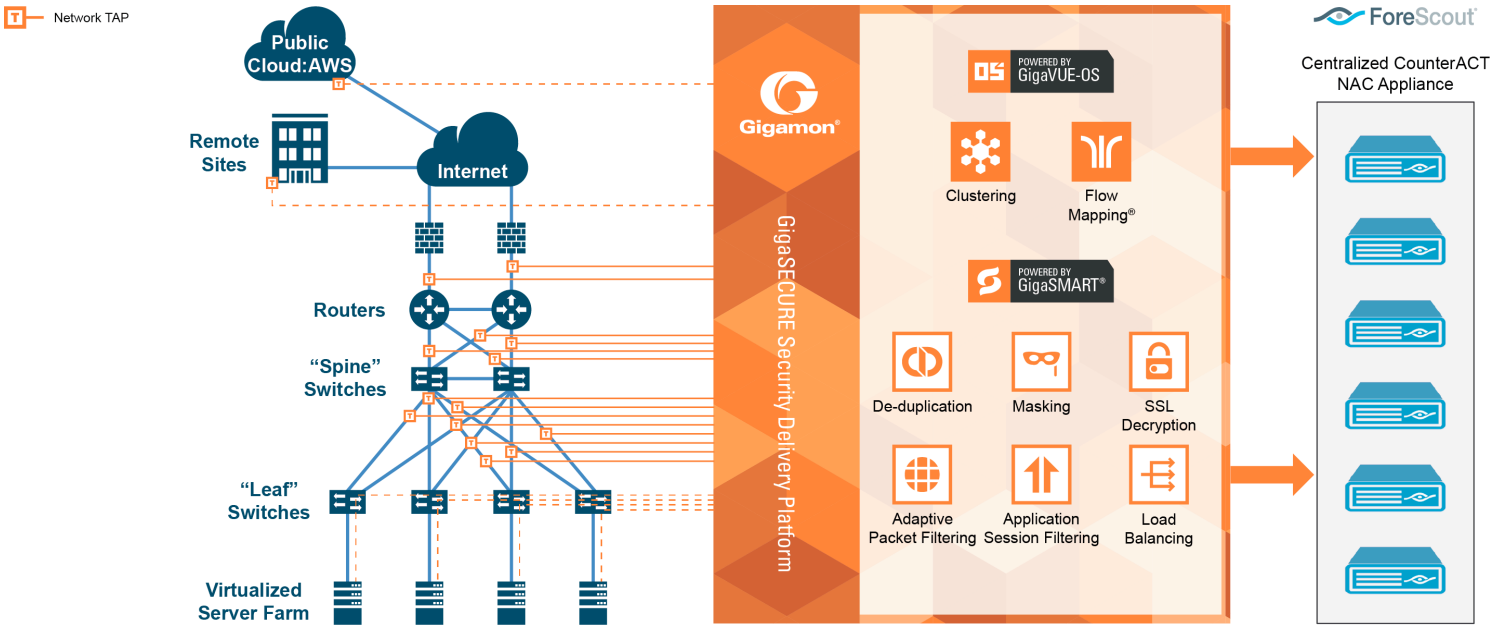
The Gigamon and ForeScout Joint Solution

ForeScout agentless technology discovers, classifies and assesses devices. It analyzes traffic and integrates with the network infrastructure to discover devices as they connect to the network. After discovering a device, ForeScout uses a combination of passive and active methods – where active inspection is acceptable – to classify the device according to its type and ownership. Based on its classification, ForeScout then assesses the device security posture and allows organizations to set policies enforcing the specific behavior the device is allowed to have while connected to a network.

The Gigamon® GigaSECURE® Security Delivery Platform provides a great complement to ForeScout by delivering efficient, resilient and scalable access to traffic from across the network.

Key features offered by the GigaSECURE platform include:

- **Scalability:** Through a combination of aggregation and load balancing across multiple ForeScout devices, an installation can be designed to help ensure maximum efficiency and scale. New ForeScout devices can be added as traffic loads increase without service interruption or unnecessary devices being required.
- **Efficiency:** By utilizing the GigaSECURE® Security Delivery Platform traffic filtering features, irrelevant network traffic can be dropped from the flows being analyzed by the ForeScout devices. Similarly, aggregated traffic flows can be deduplicated to help ensure that each packet is only analyzed by the ForeScout devices once.



- **Compliance:** For industries where certain identifiable information such as patient data or credit cards numbers cannot be disclosed to network operations teams, the GigaSECURE® Security Delivery Platform provides the ability to mask data within packets before they are forwarded to ForeScout.
- **Complete Visibility:** With more encrypted traffic traveling across the network, analyzing and identifying application level details can sometimes be challenging. The GigaSECURE® Security Delivery Platform offers the capability to decrypt appropriate network traffic and forward it to ForeScout devices for analysis before resigning and re-encrypting the traffic for onward delivery.

Learn More

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

ForeScout
www.forescout.com

Gigamon®
www.gigamon.com

3025-05 10/17