Efficiently Identify and Secure Devices with Gigamon and Forescout

Overview

A foundational element of security is knowing what's on the network and how each infrastructure device is behaving. New devices, such as unmanaged laptops, smartphones, tablets, Internet of Things (IoT) devices, and rogue devices join networks nearly every hour. The task of gaining complete visibility across all these devices for security postures has become a challenge as infrastructures migrate to the cloud and become more complex. 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 Challenge

An increasing number of devices are joining networks as organizations try to drive a better, more effective experience for customers. These devices significantly expand the attack surface and are invisible to many security tools because they are complex and often misidentified. Continuous visibility is now necessary given the risk and constant changes occurring with devices being added, removed, and relocated.

The Solution

The Forescout solution consolidates multiple feeds of intelligence from customer environments to provide visibility and control for all network-connected devices. One significant source of intelligence is network traffic. The Gigamon Deep Observability Pipeline accesses network-derived intelligence from across an entire infrastructure and sends it to the Forescout solution. Forescout combines Gigamon with other streams of intelligence for efficient identification of devices on the network.

Key Features

Forescout's agentless technology discovers, classifies, and assesses devices. Their solution analyzes traffic and integrates with network infrastructure to discover devices as they connect to the network. After discovering a device, Forescout uses both passive and active methods to classify the device according to its type and ownership. Based on its classification, Forescout assesses the device security posture

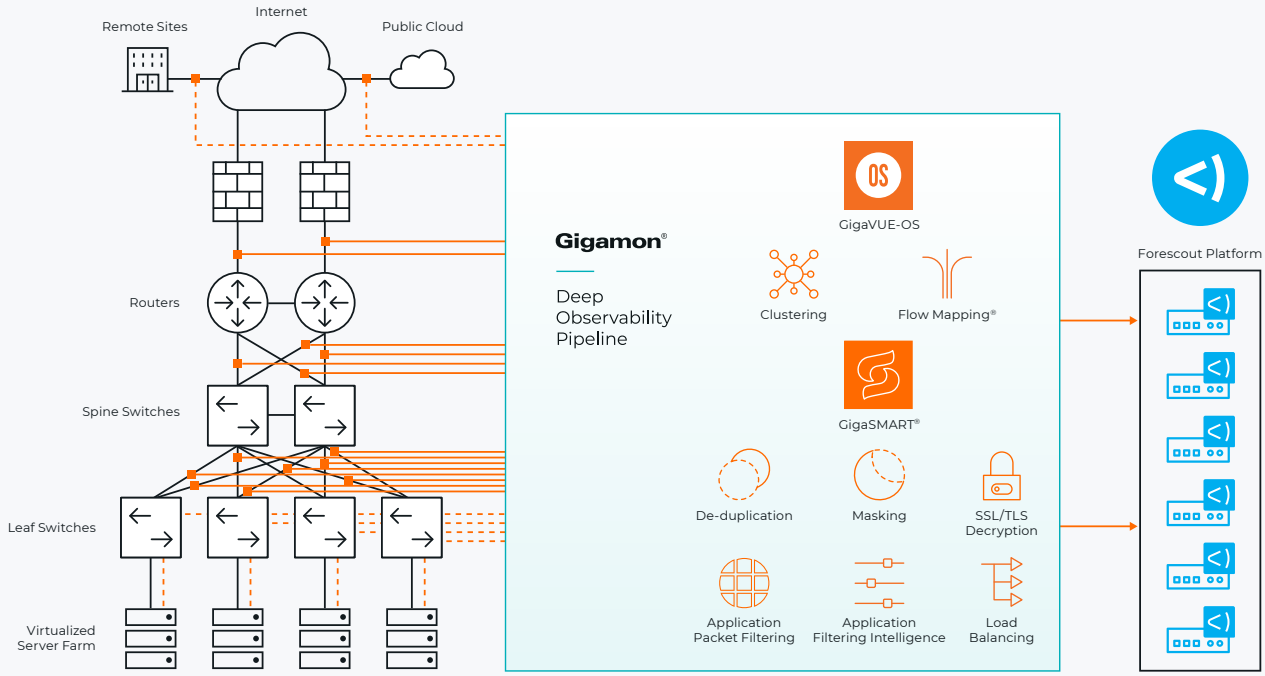

Figure 1. The Gigamon and Forescout joint solution.

and allows organizations to set policies enforcing the specific behavior the device is permitted while connected to a network.

The Gigamon Deep Observability Pipeline complements the other streams of intelligence Forescout analyzes by delivering efficient and scalable access to network-derived intelligence across the entire network.

The joint solution offers:

- **Scalability:** Organizations can ensure that all their tools, including Forescout, have complete visibility without the creation of blind spots as devices join the network and infrastructure changes occur.
- **Efficiency:** The Gigamon Deep Observability Pipeline traffic filtering features allow irrelevant network traffic to be dropped from the flows being analyzed by the Forescout Platform. Similarly, aggregated traffic flows can be de-duplicated to help ensure that each packet is analyzed only once by the Forescout Platform.
- **Compliance:** For industries where certain identifiable information, such as patient data or credit card numbers, cannot be disclosed to network operations teams, the Gigamon Deep Observability Pipeline 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 be challenging. The Gigamon Deep Observability Pipeline offers the capability to decrypt appropriate network traffic and forward it to Forescout Platform for analysis before resigning and re-encrypting the traffic for onward delivery.

About Forescout

Forescout delivers automated cybersecurity across the digital terrain. We empower our customers to achieve continuous alignment of their security frameworks with their digital realities, across all asset types — IT, IoT, OT, and IoMT. It is a nonstop journey, managing cyber risk through automation and data-powered insights.

The Forescout platform provides complete asset visibility of connected devices, continuous compliance, network segmentation, network access control, and a strong foundation for Zero Trust. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide automated cybersecurity at scale. Forescout customers gain data-powered intelligence to accurately detect risks and quickly remediate cyberthreats without disruption of critical business assets.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide.

To learn more, please visit gigamon.com.

For more information on Gigamon and Forescout please visit
gigamon.com | forescout.com

Gigamon®

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

07.23_08