Gigamon® | <) FORESCOUT

End-to-End Asset Visibility and Control for OT with Gigamon and Forescout

Overview

A foundational element of security is knowing what is on the network and how each asset is behaving. New devices, such as unmanaged laptops, smartphones, tablets, smart devices, and IoT devices, join networks nearly every hour. At the same time, operational technology (OT) environments are full of legacy systems, unmanaged switches and flat or partially segmented networks that were never designed with security in mind. Because of these challenges, organizations are looking for a flexible solution that allows them to easily access intelligence from multiple sources and centralize delivery to any analysis technology. In OT networks, this means overcoming SPAN port limitations, gaining visibility into traffic from unmanaged switches, and eliminating blind spots between control networks, safety systems, and enterprise IT. Accomplishing this minimizes blind spots, strengthens OT and IT security postures, and improves overall security hygiene.

The Challenge

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

In OT environments, this challenge is amplified:

- SPAN limitations in OT networks: Industrial and campus switches often have a number of SPAN/mirror ports or legacy devices that doesn't support that capability. Security and network teams must choose which links to monitor, leading to critical blind spots on safety, SCADA, or control system traffic and in some cases also to oversubscription and dropped packets.

- Unmanaged switches and OT devices: Many plants, substations, and remote sites rely on unmanaged Ethernet switches and network devices that provide no native telemetry or access control. Traffic between controllers, HMIs, and sensors may never reach traditional monitoring tools.
- Legacy and fragile assets: OT devices frequently cannot support agents or frequent active scans. Misconfigurations or intrusive probing can impact availability, making passive, network-based visibility essential.

As infrastructures span IT, OT, and cloud, organizations need a way to extend deep, continuous visibility across these heterogeneous environments—without overloading limited SPAN ports or disrupting sensitive OT systems.

The Solution

The Gigamon Deep Observability Pipeline accesses traffic across network distributed infrastructure and delivers network-derived telemetry to the tools an organization uses to secure and monitor performance. The Forescout platform consolidates multiple feeds of data from customer environments to provide asset intelligence and control for all network-connected assets. Forescout combines Gigamon with other streams of intelligence for efficient identification of assets on the network. For OT environments, Gigamon and Forescout together to:

- Aggregate and optimize traffic from SPAN ports, hardware taps, and unmanaged switches so that no critical OT segment is left unmonitored—even when SPAN capacity is constrained.
- Offload and centralize packet processing (de-duplication, filtering, masking, and TLS/SSL decryption) so that limited SPAN resources are used efficiently and Forescout receive only the traffic they need.
- Provide a unified view of data in motion across IT, OT, private and public cloud, and containers, enabling consistent policy enforcement and faster incident response in mixed environments.

By inserting the Gigamon Deep Observability Pipeline between OT network infrastructure (SPANs and taps) and the Forescout platform, organizations can overcome physical monitoring constraints and extend deep asset intelligence into industrial and critical infrastructure environments.

Key Features

Forescout's agentless technology identifies, protects, and ensures compliance of all assets. It analyzes traffic and integrates with network infrastructure to discover assets as they connect to the network. After discovering an asset, Forescout uses both passive and active methods to classify the device according to its type and ownership. Based on its classification, Forescout assesses the asset's security posture and allows organizations to set policies enforcing the specific behavior the asset is permitted while connected to a network.

The Gigamon Deep Observability Pipeline complements the other streams of intelligence Forescout analyzes by offering a unified view of data in motion across hybrid or multi-cloud infrastructures, as well as OT and industrial networks. It efficiently gathers data from multiple sources, optimizes it automatically, and delivers it seamlessly to the Forescout Platform.

The joint solution offers:

- **Scalability across IT and OT:** Organizations can ensure that all their tools, including Forescout, have complete visibility without the creation of blind spots as assets join the network and as infrastructure changes occur—even when OT switches provide limited SPAN capacity and when remote sites rely on unmanaged switches or devices. It match also the network infrastructure connectivity with Forescout platform.
- **Efficiency of constrained SPAN resources:** The Gigamon Deep Observability Pipeline can filter irrelevant network traffic from the flows analyzed by the Forescout Platform, and aggregated traffic flows can be de-duplicated to help ensure that each packet is analyzed only once. This allows security teams to make the most of scarce SPAN ports in OT networks, reducing the need for additional hardware upgrades while still feeding Forescout with complete, high-quality telemetry.

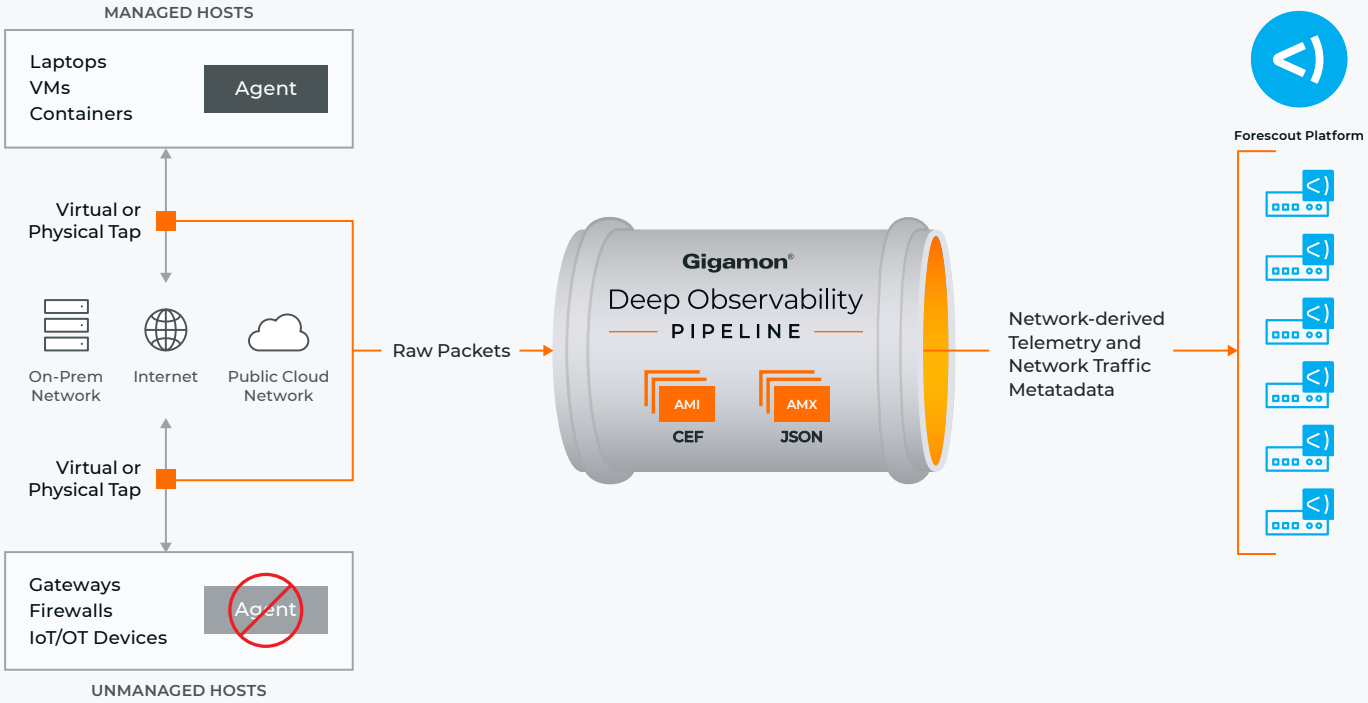

Figure 1. The Gigamon and Forescout joint solution.

- **Compliance and data protection in industrial environments:** For industries where certain identifiable information, such as factory information, airplane plan or engine diagram, cannot be disclosed to network operations teams, Gigamon provides the ability to mask data within packets before forwarding them to Forescout. This same capability can be applied to protect sensitive industrial process data while still enabling rich monitoring and threat detection.
- **Complete Asset Intelligence for OT:** With more encrypted traffic traveling across the network, analyzing and identifying application details can be challenging. The Gigamon Deep Observability Pipeline offers the capability to decrypt appropriate network traffic and forward it to the Forescout platform for analysis before re-encrypting the traffic for onward delivery. Combined with Forescout's agentless discovery and classification, this provides deep visibility into managed and unmanaged OT assets—from PLCs and RTUs to engineering workstations and HMIs—even when they sit behind unmanaged switches or out-of-band taps.

About Forescout

Forescout Technologies, Inc., a global cybersecurity leader, continuously identifies, protects and helps ensure the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide vendor-agnostic, automated cybersecurity at scale.

The Forescout Platform delivers comprehensive capabilities for network security, risk and exposure management, and threat detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats.

About Gigamon

Gigamon® delivers an AI-powered Deep Observability Pipeline that provides network-derived telemetry to cloud, security, and observability tools. With AI-driven insights across packets, flows, and application metadata, organizations gain complete visibility into all data in motion to detect threats concealed in encrypted and lateral traffic, resolve network and application performance issues, and validate compliance while reducing operational cost and complexity. Gigamon is trusted by 4,000+ organizations, including 83 of the Fortune 100 and hundreds of public sector agencies and educational institutions. Learn more at 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

02.26_11