JOINT SOLUTION BRIEF
GIGAMON AND ORDR

Comprehensive IoT, IoMT and OT Device Visibility, Discovery, Classification and Security

IoT And OT Are Expanding Faster Than They Can Be Secured

The number of IoT and other connected devices is exponentially increasing on enterprise networks, often without knowledge of their connection, location, specific purpose, or security team awareness. These devices present unique challenges to discovery, risk assessment, and security as they typically access the network without authentication or an associated user. Many connected devices – particularly IoMT, OT, and ICS devices – are highly vulnerable, often running rudimentary or minimized versions of legacy operating systems without basic client protection software. Additionally, they are commonly closed, proprietary systems with minimal or no patching capabilities to defend themselves meaning that installation of security or device management software is rarely an option.

The bottom-line is that, despite their operational benefits, IoT, IoMT, and OT devices introduce security vulnerabilities and visibility blind spots that significantly increase risks that can result in service disruption, data theft, or compromise leading to ransomware and other attacks.

Take Control of Your Enterprise

The basic tenet of security is that "you cannot secure what you cannot see." Gigamon and Ordr have teamed to deliver complete visibility and control into everything connected to your infrastructure including unmanaged workstations and servers, medical and industrial devices, building automation systems, smart branches and offices, payment processors in PCI zones, as well as the wide variety of other connected devices increasingly found on enterprise networks.

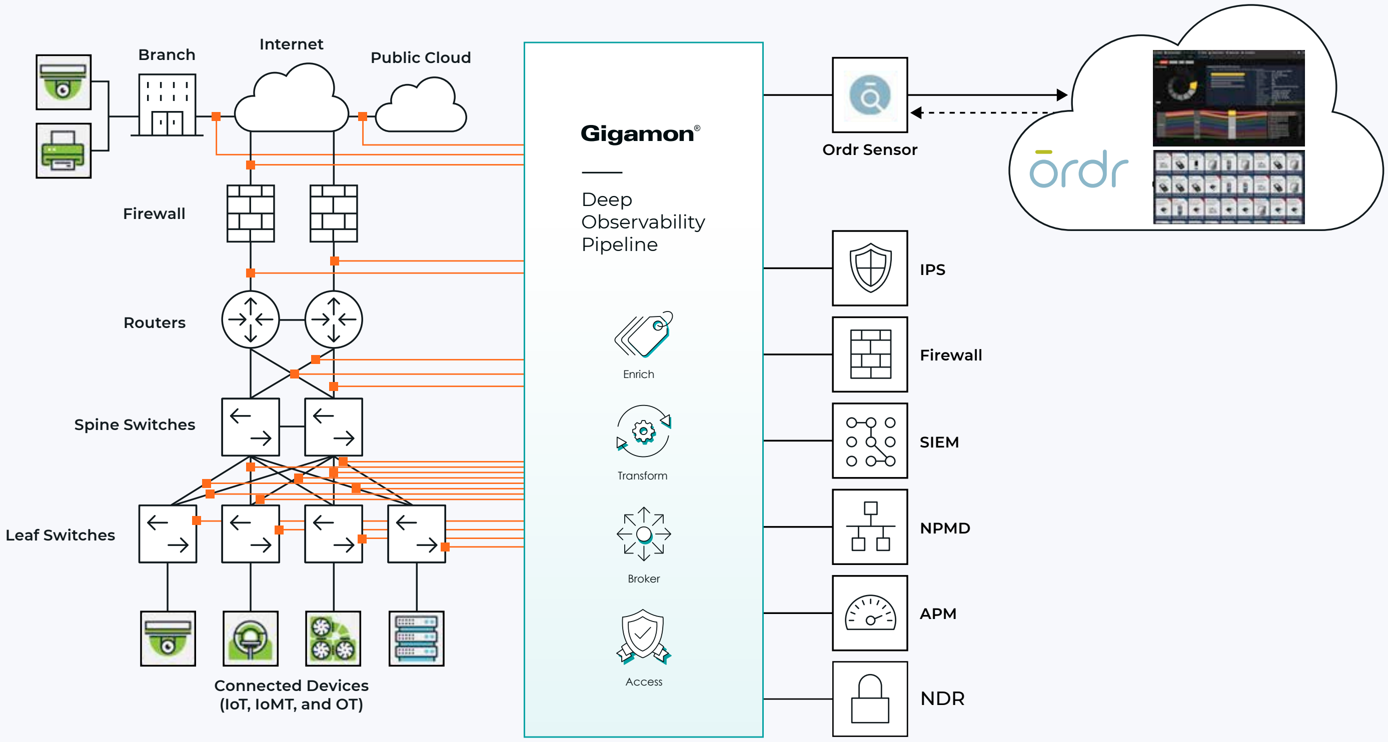
GIGAMON DEEP OBSERVABILITY PIPELINE

- Efficiently collects high-fidelity, data-in-motion from your hybrid-cloud infrastructure including East-West and Encrypted data
- Aggregates traffic to create a consistent, complete view of data-in-motion
- Optimizes traffic sent to network, security and observability tools to maximize their efficiency and ROI
- Transforms traffic using techniques including de-duplication, advanced filtering and metadata generation
- Eliminates the limitations of using SPAN ports and Cloud Mirroring to collect data-in-motion to enable complete monitoring and deep observability
- Supports centralized TLS decryption, ensuring visibility into encrypted payloads and relieving load on firewall

ORDR CONNECTED DEVICE SECURITY

- Passively discovers all connected devices by analyzing device traffic from sources such as Gigamon
- Automatically and accurately classifies devices with granular details
- Identifies security vulnerabilities, active threats, and calculates a risk score for each device
- Learns device behaviors to establish baselines of normal communication and enables quick detection of anomalous activity
- Automates policy to mitigate risks during an attack by quarantining devices, blocking traffic, or terminating sessions, and proactively improves security with policy for Zero Trust segmentation and NAC

The Solution

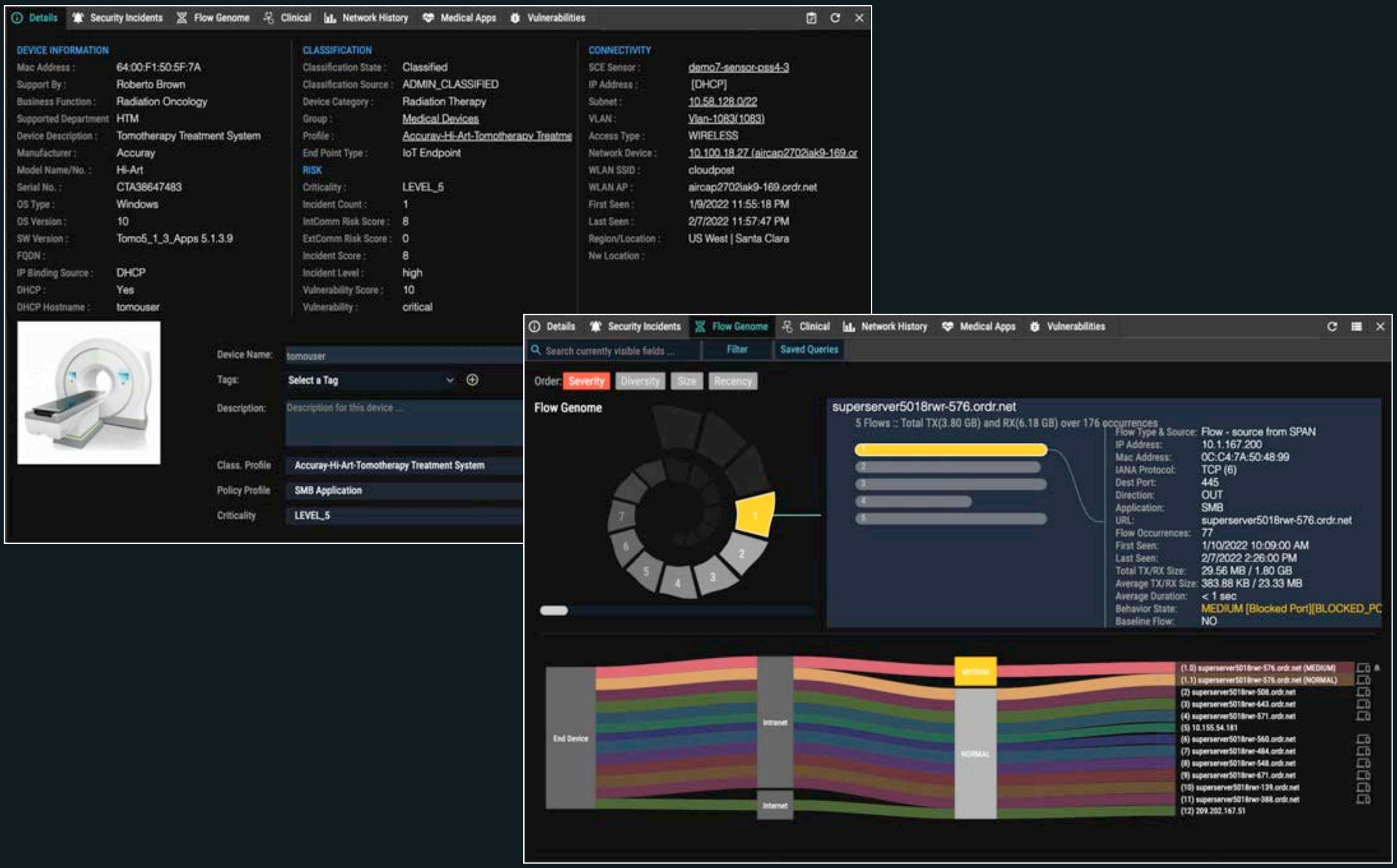


Total Device Visibility And Security

Ordr is the industry's most comprehensive platform for visibility and security of all connected devices. Ordr leverages passive, deep packet inspection and protocol decoding to automatically classify every device and extract rich context such as make, model, OS, and software/hardware versions. Device asset inventory is correlated against industry security feeds to detect vulnerabilities, and traffic is monitored to detect threats, assess risk, and establish baselines for normal and safe device communications. Device baselines enable Ordr to alert on anomalous behavior, automate response, and dynamically generate micro segmentation policies to protect critical connected devices.

To ensure accurate device classification and comprehensive visibility into all device communications, it is essential to have complete, consistent high-fidelity traffic collection across the network. The Gigamon Deep Observability Pipeline optimizes collection of data-in-motion for all North-South, East-West and encrypted traffic across an organization's hybrid infrastructure. This data is aggregated, transformed, and optimized before being delivered to Order, establishing complete visibility into all connected devices and device communications. Gigamon also eliminates SPAN and Cloud Mirroring performance and inefficiency issues using both physical and virtual taps that scale to ensure high-fidelity data is collected and aggregated across an entire hybrid infrastructure regardless of scale. This approach enables Gigamon to significantly reduce the number of sensors required to discover and monitor every device connected to your infrastructure, simplifying your network and security monitoring architecture.

ORDR ANALYZES DATA-IN-MOTION CAPTURED AND OPTIMIZED BY THE GIGAMON DEEP OBSERVABILITY PIPELINE TO PROVIDE HIGH-FIDELITY DEVICE CONTEXT…



DEVICE INFORMATION
Mac Address : 64:00:F1:50:5F:7A
Support By : Roberto Brown
Business Function : Radiation Oncology
Supported Department HTM
Device Description : Tomotherapy Treatment System
Manufacturer : Accuray
Model Name/No. : Hi-Art
Serial No. : CTA38647483
OS Type : Windows
OS Version : 10
SW Version : Tomo5_1_3_Apps 5.1.3.9
FQDN :
IP Binding Source : DHCP
DHCP : Yes
DHCP Hostname : tomouser

CLASSIFICATION
Classification State : Classified
Classification Source : ADMIN_CLASSIFIED
Device Category : Radiation Therapy
Group : Medical Devices
Profile : Accuray-Hi-Art-Tomotherapy Treatme
End Point Type : IoT Endpoint

RISK
Criticality : LEVEL_5
Incident Count : 1
IntComm Risk Score : 8
ExtComm Risk Score : 0
Incident Score : 8
Incident Level : high
Vulnerability Score : 10
Vulnerability : critical

CONNECTIVITY
SCE Sensor : demo7-sensor-pss4-3
IP Address : [DHCP]
Subnet : 10.58.128.0/22
VLAN : Vlan-1083(1083)
Access Type : WIRELESS
Network Device : 10.100.18.27 (aircap2702iak9-169.or
WLAN SSID : cloudpost
WLAN AP : aircap2702iak9-169.ordr.net
First Seen : 1/9/2022 11:55:18 PM
Last Seen : 2/7/2022 11:57:47 PM
Region/Location : US West | Santa Clara
Nw Location :

Device Name: tomouser
Tags: Select a Tag
Description: Description for this device ...
Class. Profile Accuray-Hi-Art-Tomotherapy Treatment System
Policy Profile SMB Application
Criticality LEVEL_5

superserver5018rwr-576.ordr.net
5 Flows :: Total TX(3.80 GB) and RX(6.18 GB) over 176 occurrences

Flow Type & Source: Flow - source from SPAN
IP Address: 10.1.167.200
Mac Address: 0C:C4:7A:50:48:99
IANA Protocol: TCP (6)
Dest Port: 445
Direction: OUT
Application: SMB
URL: superserver5018rwr-576.ordr.net
Flow Occurrences: 77
First Seen: 1/10/2022 10:09:00 AM
Last Seen: 2/7/2022 2:26:00 PM
Total TX/RX Size: 29.56 MB / 1.80 GB
Average TX/RX Size: 383.88 KB / 23.33 MB
Average Duration: < 1 sec
Behavior State: MEDIUM [Blocked Port][BLOCKED_PC
Baseline Flow: NO

(1.0) superserver5018rwr-576.ordr.net (MEDIUM)
(1.1) superserver5018rwr-576.ordr.net (NORMAL)
(2) superserver5018rwr-508.ordr.net
(3) superserver5018rwr-643.ordr.net
(4) superserver5018rwr-571.ordr.net
(5) 10.155.54.181
(6) superserver5018rwr-560.ordr.net
(7) superserver5018rwr-484.ordr.net
(8) superserver5018rwr-548.ordr.net
(9) superserver5018rwr-671.ordr.net
(10) superserver5018rwr-139.ordr.net
(11) superserver5018rwr-388.ordr.net
(12) 209.202.167.51

…AND COMPLETE VISIBILITY INTO ALL DEVICES AND DEVICE COMMUNICATIONS.

Gigamon And Ordr Use Cases

- Real-time asset inventory – Ordr continuously analyzes device traffic sent from Gigamon to passively discover and automatically classify every device connected to the network to help you maintain an up-to-date and accurate inventory.
- Medical device utilization – Ordr provides detailed medical device utilization insights for high-capital equipment to help inform maintenance tasks and capital purchase decisions.
- Connected device risk – using the traffic captured and optimized by the Gigamon Deep Observability Pipeline, Ordr calculates device risk scores and uncovers connected devices with risk such as outdated operating systems, unpatched software, weak passwords, and manufacturer recalls. Ordr also maps and baselines device communications to identify risk and stop attacks.
- Accelerate Zero Trust – working together, Gigamon and Ordr can map and baseline all IT, IoT and other device communications. Ordr can then dynamically create Zero Trust policies to simplify and accelerate NAC and segmentation projects. These policies can be enforced with popular security and network devices to integrate with existing infrastructure tools.

Summary

The Gigamon Deep Observability Pipeline provides access to all the data-in-motion across an organization's hybrid infrastructure and enables Ordr to keep track of all your connected devices, understand how they communicate, and improve security. The Gigamon Deep Observability Pipeline aggregates, transforms and optimizes data-in-motion before routing it to Ordr ensuring that it can be processes quickly and efficiently. Gigamon and Ordr can be deployed in physical or virtual data centers or in the public cloud and work together seamlessly to ensure organization-wide visibility and security of connected devices.

Numerous customers across all industries already deploy the joint Gigamon and Ordr solution in their networks, enjoying unparalleled network and device visibility and control. For more information or to see a demonstration, please contact your reseller.

ABOUT ORDR

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing Venture Capital, Ten Eleven Ventures, Northgate Capital, Kaiser Permanente Ventures, and Unusual Ventures. For more information, visit ordr.net and follow Ordr on Twitter and LinkedIn.

ABOUT GIGAMON

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables 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, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

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