APPLICATION NOTE

Forescout eyeInspect on the iROC Module

INTRODUCTION

The ongoing convergence of information technology (IT) and operational technology (OT) networks is increasing the complexity and vulnerability of previously isolated industrial control system (ICS) networks. This is taking place alongside the explosive growth of Industrial IoT (IIoT) devices, which has created a significant visibility gap and made compliance enforcement more difficult. Organizations need a security tool that can provide in-depth visibility into OT and ICS networks and enable effective, real-time management of operational and cyber risks.

Forescout eyeInspect provides in-depth device visibility for OT networks and enables effective, real-time management of a full range of operational and cyber risks.

The eyeInspect solution has been integrated into iS5Com's leading edge RAPTOR® iMX350 & iMX950 models to offer a cost effective and flexible solution.

Forescout eyeInspect

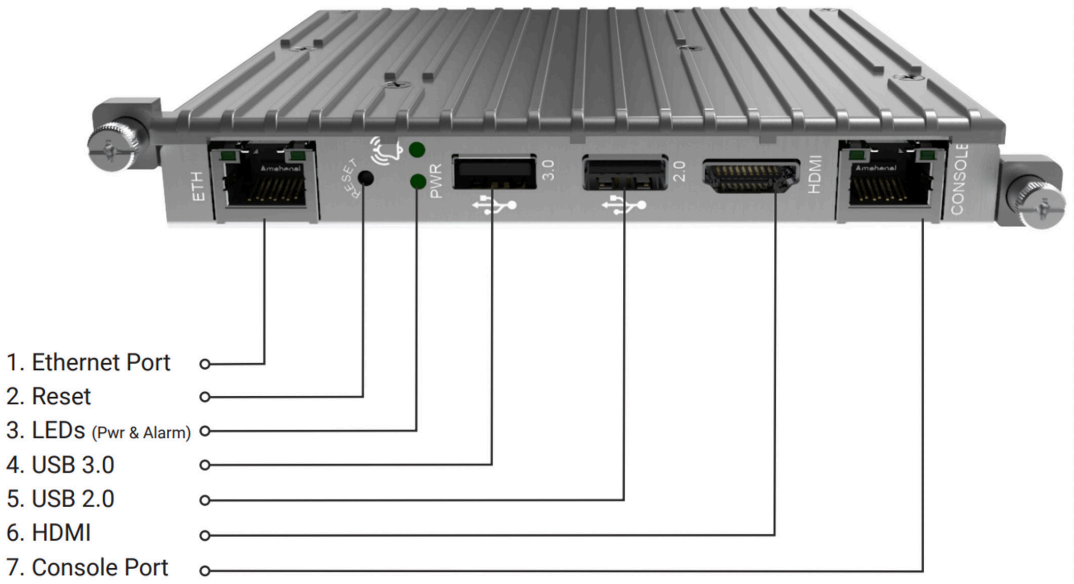
Forescout eyeInspect (formerly SilentDefense™) protects OT and ICS networks from a wide range of threats, provides both passive and active discovery capabilities that create an automatic, real-time asset inventory and enables targeted remediation actions based on potential business impact.

- **Enables passive, real-time network monitoring and segmentation**
- **Optimizes threat analysis and remediation with the Advanced Alert Aggregation**
- **Offers rich integrations with ServiceNow® and natively interfaces with SIEM solutions, firewalls, IT asset management, sandboxes and authentication servers**
- **Improves SOC and analyst effectiveness to automate risk analysis with the Asset Risk Framework**
- **Extends the exceptional device visibility, classification and profiling capabilities of the Forescout platform from cloud to edge devices**

iROC Module

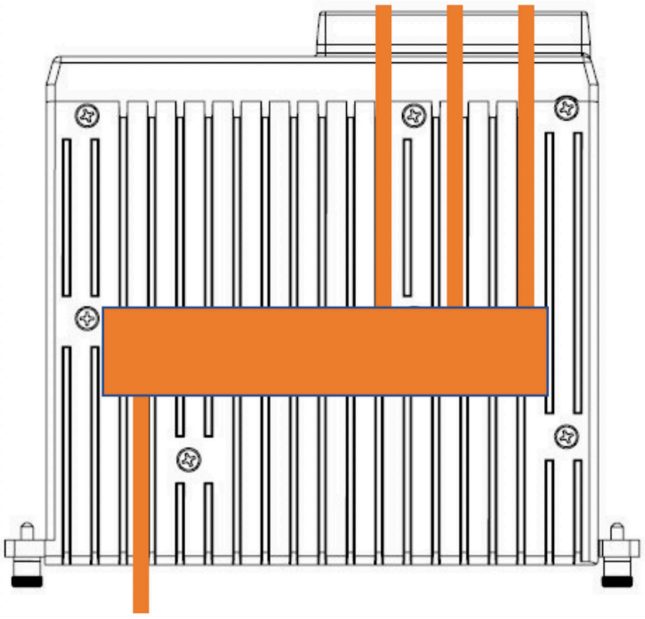
The iROC computing module is a hot-swappable industrial computing module that can be inserted into slots 1 through 4 of the RAPTOR iMX350.

Figure 1 - *iROC Front View*



The iROC supports up to three network connections through its backplane and one on its faceplate. The interfaces are 1Gbps, however they will have an effective throughput of less than 1Gbps based on factors such as CPU load, operating system, and other system demands.

Figure 2 - *iROC Backplane Interfaces*



The three backplane ports of the iROC are connected to switch fabric internal ports. The table below shows the mapping between the iROC module ports and the switch fabric based on the slot number where the iROC is inserted.

Table 1 - *iROC and RAPTOR Ports Mapping*

iROC Location	Port 1	Port 2	Port 3
Line Module 1	Gi0/1	Gi0/5	
Line Module 2	Gi0/9	Gi0/13	
Line Module 3	Gi0/17	Gi0/21	
Line Module 4	Ex0/1	Ex0/3	Ex0/4

eyeInspect Deployment Architecture

An eyeInspect deployment consists of a Command Center and one or more Passive Sensors.

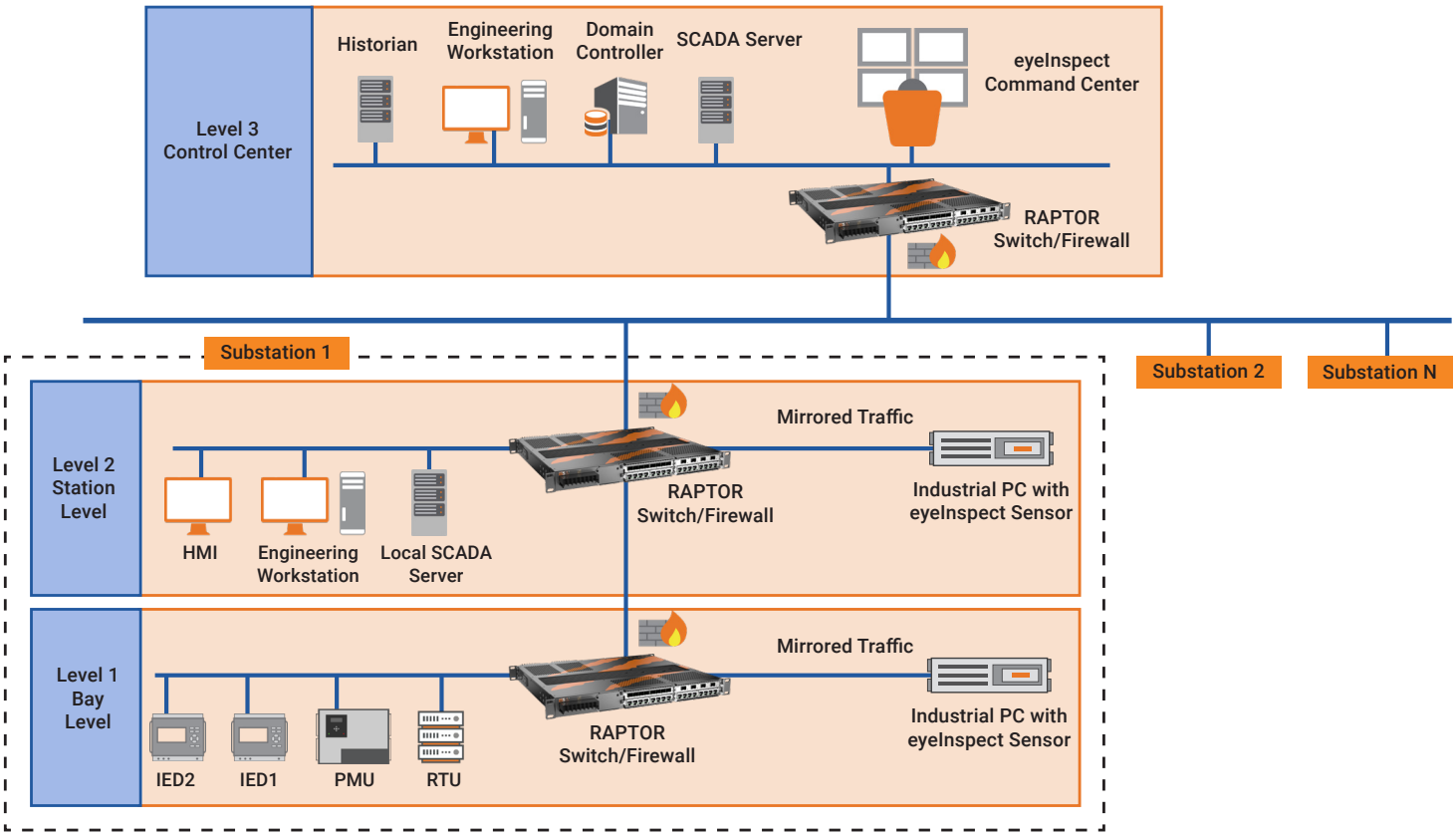
A Passive Sensor is connected to the ICS/SCADA network via a SPAN/mirroring port to passively listen to the network traffic. A Passive Sensor has several self-configuring detection engines and detection levels. Each Passive Sensor has one or more network interfaces for monitoring (i.e. monitoring ports) and a management interface. Passive Sensors send events and logs to the Command Center via the management interface.

The Sensor is installed in an industrial PC and connected to the ICS/SCADA network via a span/mirroring port to passively listen to network traffic.

The Command Center is a web-based application used for sensor and event management and provides visual representations and analysis capabilities for logs and events. The Command Center can interface with several third-party enterprise systems, e.g. a SIEM system.

Figure 3 represent the architecture of a deployment for a substation network.

Figure 3 - eyeInspect Architecture



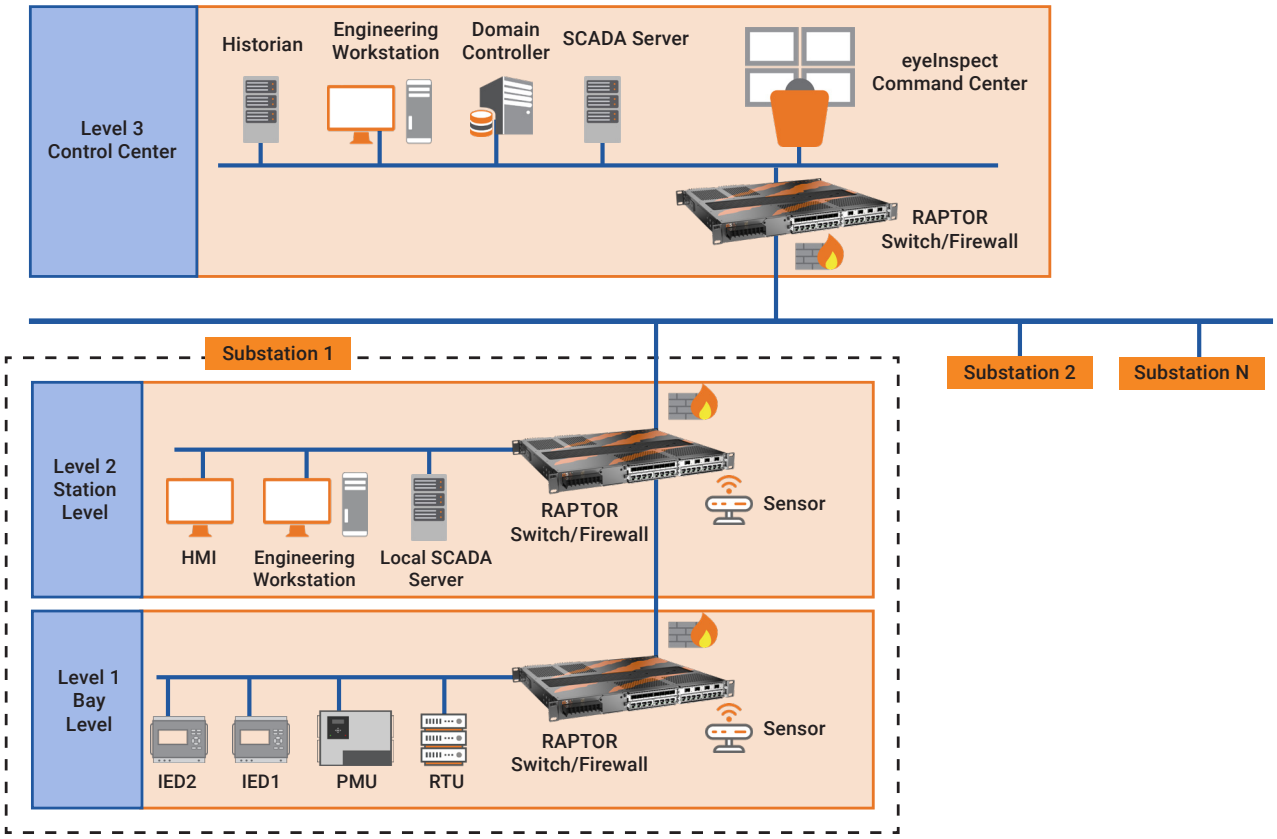
eyeInspect Architecture with the iROC Module

Most modern industrial network designs segment the network based on the Purdue model. Multiple levels (or zones) are created and the communication between zones is restricted. Mirrored traffic cannot cross zones. Therefore, a sensor interface is required at each level. This design is simplified by integrating the IDS sensor into RAPTOR. The Sensor is running on the iROC module, and it receives the mirrored traffic from the switch fabric of the RAPTOR.

This flexible design reduces the space needed in the cabinet and simplifies the hardware deployment by eliminating the need for a dedicated industrial PC and the cables between the PC and the switch.

Figure 4 represents the architecture of a deployment for a substation network with the IDS sensor integrated into the RAPTOR.

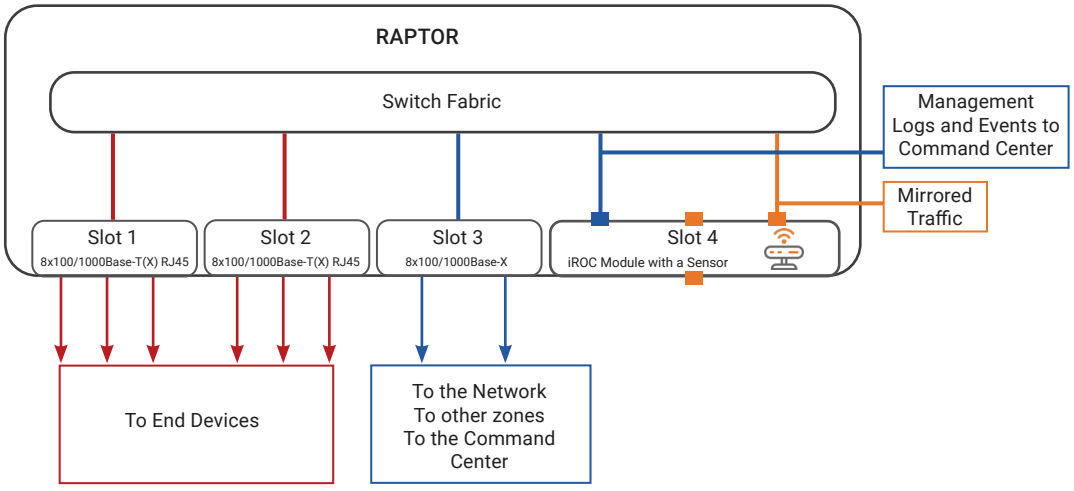
Figure 4 - eyeInspect Architecture with iROC



The traffic is mirrored by the switch and sent to the backplane interfaces of the iROC. One backplane interface is used to manage the sensor through SSH and to send the logs and events to the command center. The command center is also monitoring and collecting the sensor performance metrics and alarms through the backplane management interface. One backplane interface can be used to receive the mirrored traffic for analysis.

Up to 150 Mbps of traffic can be analyzed by the sensor when running on iROC. Figure 5 shows the internal architecture of the RAPTOR with the iROC on slot 4.

Figure 5 - RAPTOR Internal Connections



Installation and Configuration

The Forescout sensor comes preinstalled in the iROC module. Four steps are required to configure the Sensor.

1. **Insert the iROC in any slot of the RAPTOR**

   It is preferred to use slot 4 to have three backplane interfaces. Slot 1 to 3 will have two backplane interfaces.

2. **Login to the sensor**

   To connect to the iROC, connect a PC to any port of the RAPTOR and open a terminal emulation window that supports either Telnet or SSH client, such as TeraTerm or PuTTY.

   The default IP address is 192.168.10.10

   The default username and password are set as:

   Username: eyeInspect

   Password: eyeInspect

3. **Use the SDConfig tool to configure the management interface**

   Refer to the Forescout installation and configuration guide.

4. **Use SDconfig tool to select the monitoring interfaces.**

   Refer to the Forescout installation and configuration guide.

The configuration below can be used to send all ingress and egress traffic of port Gi 0/3 to the third port of the iROC module when inserted in slot 4. Refer to table 1 to see the mapping between the RAPTOR internal ports and iROC ports based on the slot number.

1. **Enable port mirroring**

   is5com(config)# set mirroring enable

2. **Configure port mirroring. Mirror the incoming and outgoing traffic of port Gi 0/3 to port Ex 0/4**

   iS5com(config)# monitor session 1 source interface gi 0/3 both

   iS5com(config)# monitor session 1 destination interface ex 0/4

3. **Verify the configuration**

   is5com(config)# show monitor session 1

CONCLUSION

By integrating the eyeInspect sensor into the RAPTOR platform with the iROC module, iS5Com offers an industrial grade flexible and scalable solution that reduces the cost, space, complexity, and time to deploy the Forescout eyeInspect solution. By integrating the eyeInspect sensor into the RAPTOR platform with the iROC module, iS5Com offers an industrial grade (IEC 61850 & IEEE 1613 compliant) flexible and scalable solution that reduces the cost, space, complexity, and time to deploy the Forescout eyeInspect solution.

eyeInspect extends the industry leading device visibility, classification and profiling capabilities of the Forescout platform far deeper into OT and ICS environments. It enables the identification and effective remediation of a full range of both cyber and operational threats.

ABOUT iS5 COMMUNICATIONS INC.

iS5 Communications Inc. ("iS5Com") is a global provider of integrated services and solutions, and manufacturer of intelligent Industrial Ethernet products. Our products are designed to meet the stringent demand requirements of utility sub-stations, roadside transportation, rail, and industrial applications. iS5Com's services and products are key enablers of advanced technology implementation such as the Smart Grid, Intelligent Transportation Systems, Intelligent Oil Field, and Internet of Things. All products have the ability to transmit data efficiently without the loss of any packets under harsh environments and EMI conditions.

iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

For more information, visit: is5com.com

toll free: +1-844-520-0588 | fax: +1-289-401-5206 | info@is5com.com
technical support: +1-844-475-8324 | support@is5com.com
Address: 5895 Ambler Dr, Mississauga, ON L4W 5B7