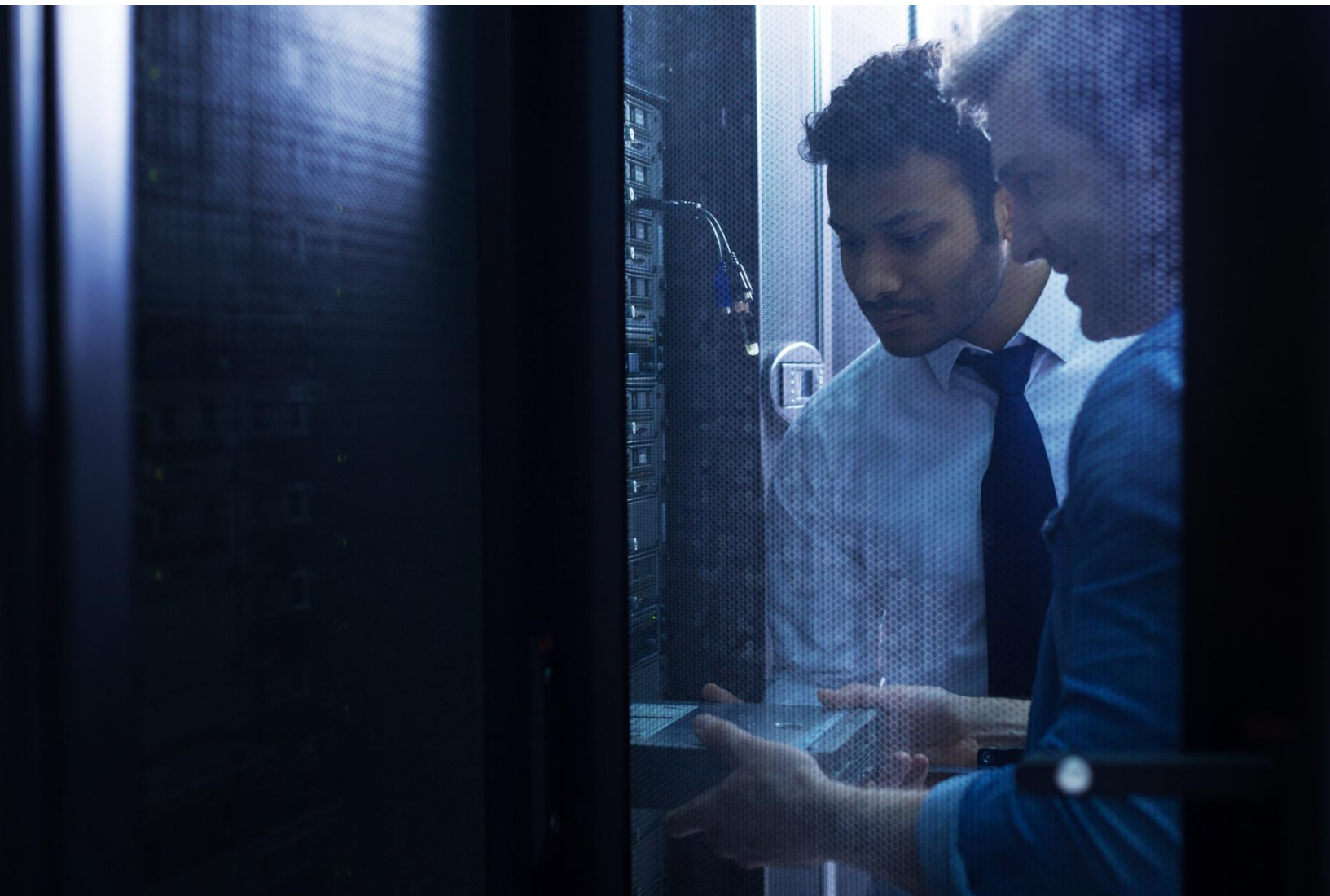




# Forescout OT Hardware Guidelines

September, 2021

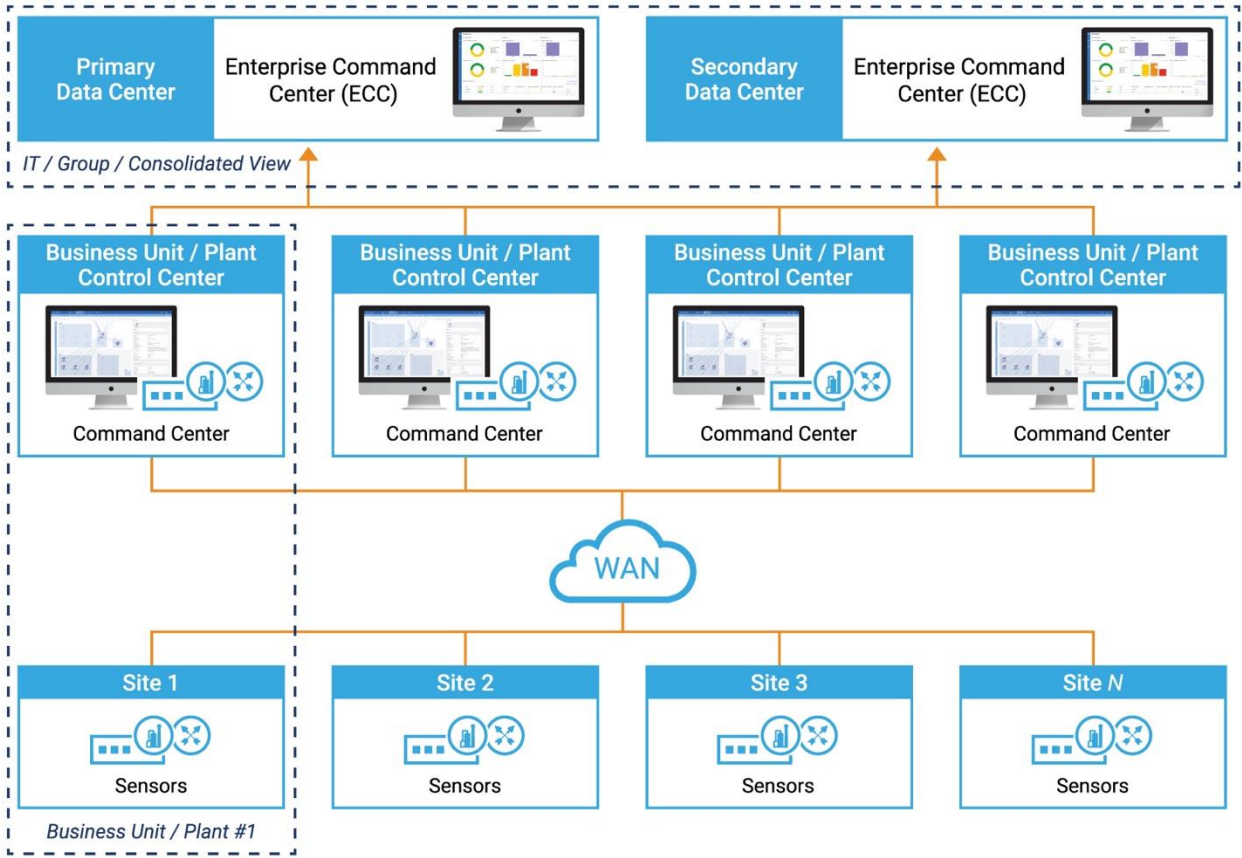


- Introduction ..... 2**
- 1.0 Enterprise Command Center ..... 3**
- 2.0 Command Center ..... 3**
  - 2.1 eyeInspect Command Center Requirements ..... 4*
  - 2.2 eyeSight Command Center Requirements..... 5*
- 3.0 Sensors ..... 6**
  - 3.1 Passive Monitoring Sensor Requirements ..... 6*
  - 3.2 Active Sensor Requirements ..... 8*
- 4.0 Qualified Hardware Appliances ..... 9**
  - 4.1 Rack server — Dell® PowerEdge R640 ..... 9*
  - 4.2 Rack server — Forescout® 5120, 5140, 5160 ..... 12*
  - 4.3 Short-depth rack server — Supermicro SuperServer E300-9A-4CN10P ..... 13*
  - 4.4 Industrial PC — Forescout® 4130 ..... 14*
  - 4.5 Industrial PC — Schweitzer Engineering Laboratories® SEL-3350..... 15*
  - 4.6 Industrial PC — Schweitzer Engineering Laboratories® SEL-3355..... 16*
  - 4.6 DIN-Rail industrial PC — FoxGuard® Solutions IADIN-FS1..... 17*

# Introduction

Forescout eyeInspect offers a 3-tier architecture with Passive or Active Monitoring Sensors, Command Centers (CC), and Enterprise Command Centers (ECC) allowing for large deployments.

A basic deployment consists of a Command Center (CC) and one or more Sensors. A CC is commonly installed per site, plant or business unit. An Enterprise Command Center (ECC) can be deployed to provide central or regional OT visibility and threat detection insights connecting to one or more Command Centers.



Sensors monitor live network traffic via mirroring/SPAN port(s) or physical tap(s). Sensor density, placement, and form factor selection is very important. Your Forescout Systems Engineer can provide guidance for meeting the needs of your specific environment. The options you see in this document represent hardware options for Command Centers and Sensors. Some environments have adequate space, environmental controls, and rack availability for 1-3U rack server appliances. However, in many OT environments, this is not the case. The non-rack mount and ruggedized models shown in this guide provide solutions for harsh environments.

Sensor selection involves taking multiple variables into account, such as: physical space available, power supply limitations, required operating temperature range, endpoint session count, monitored traffic throughput needs, etc. Please consult with your Forescout account team for guidance to create an architecture best suited for your environment.

In this guideline, Reference models are hardware configurations that are qualified by Forescout for deploying eyeInspect Command Centers or Sensors. Reference models are a great option for customers requiring a hardware model that is not available among the Forescout branded options. Reference models can be ordered pre-installed with the eyeInspect software through Forescout, instead of sourcing it directly from different manufacturers. “(Reference model)” will be noted next to the Forescout Part Number. Please note the manufacturers of Reference models can change their product roadmap, alternate components, and warranty offerings at any time.

## 1.0 Enterprise Command Center

The ECC is an optional component for the eyeInspect Suite. It provides a high-level view of the status of the entire OT infrastructure and facilitates deployments in large, complex organizations with multiple chains of responsibility for the management of security information. The ECC can be installed on a physical or virtual appliance and the software is compiled for the x86-64 architecture.

Minimum Requirements	
Hardware / Hypervisor	19" rack server or minimum VMware ESXi 5
Processor	4-core (Intel®) CPU 64 bits ≥ 2.4GHz or better
Memory size	≥ 16-32 GB
Hard drive	≥ 250 GB thin provisioning
Network interface #1	Interface for Command Center communication, web application access and SSH access

## 2.0 Command Center

The Command Center is a web-based management interface that can be installed on a physical or virtual appliance, with its software being compiled for the x86-64 architecture. The CC is available in two license levels – eyeInspect (hereafter referred to as eyeInspect CC), and eyeSight (hereafter referred to as

eyeSight CC). The eyeSight CC supports a subset of features as compared to the eyeInspect CC. The eyeSight CC supports asset inventory and OT vulnerabilities. The eyeInspect CC supports many additional features such as a Dashboard, Network Map, Network Analytics, Anomaly Detection, Event management, etc.

The protocols and amount of monitored traffic as well as the number of connected sensors can affect the performance requirements on the Command Center components. The following sections discuss the hardware requirements and tested systems.

## 2.1 eyeInspect Command Center Requirements

This section specifies the guidelines for the eyeInspect Command Center which can be deployed on a rack server or virtualized on VMware ESXi.

Alerts and network analytics data are stored in the CC. A larger disk allows storing the data for a longer period. Part of the network analytics data is loaded in memory. In addition, the number of sensors connected to the CC increase the memory and CPU requirements.

As minimum requirements for Hypervisor, CPU and storage, we suggest the following specification:

	Small deployment (≤5 sensors)	Medium deployment (≤20 sensors)	Large deployment (≤100 sensors)
Hardware / Hypervisor	19" rack server or minimum VMware ESXi 5		
Processor	4-core CPU 64bits	8-core CPU 64bits	16-core CPU 64bits ≥ 2.4GHz or better
Hard drive	500GB	1TB	>1TB
	(Based on data retention of 90 days)		
Network interface #1	Interface for sensor communication, web application access and SSH access		

For memory (RAM) guidelines, usage depends on several parameters. The most relevant are:

- The number of Sensors connected to the Command Center.
- The average of the observed network traffic throughput considering the contribution of each Sensor connected.
- The amount of network hosts in the network.

- d) Number of network events per second, such as: authentication/encryption events, file operations, name resolutions, potentially dangerous operations and traffic flow information.

However, parameters b), c), and d) above are not always known. The table below suggests the memory requirements based on the number of Sensors connected to the Command Center and total network throughput (measured in terms of events per second received by the Command Center).

	Memory Requirement	Network Events per Second
Up to 10 Monitoring Sensors	64 GB	1200 network events/sec
Up to 20 Monitoring Sensors	128 GB	2400 network events/sec
Up to 100 Monitoring Sensors	256 GB	4800 network events/sec

## 2.2 eyeSight Command Center Requirements

This section specifies the guidelines for the eyeSight Command Center deployed with Forescout eyeSight, which supports asset inventory and vulnerability discovery.

The Command Center can be installed on a rack server or virtualized on VMware ESXi. As general guidelines we suggest the following specification\*:

Minimum Requirements	
Hypervisor	minimum VMware ESXi 5
Processor	4-core (Intel®) CPU 64 bits ≥ 2.4GHz or better
Memory size	16-80 GB (see table below)
Hard drive	50 GB thin provisioning
Network interface #1	Interface for sensor communication, web application access and SSH access

The Command Center Memory usage in Forescout eyeSight depends on several parameters, the most relevant are:

- a) The number of Monitoring Sensors connected to the Command Center

- b) The average of the observed network traffic throughput taking into account the contribution of each sensor connected
- c) The amount of network hosts in the network

However, parameters b) and c) are not always known. The table below suggests the memory requirement based on the number of Monitoring Sensors connected to the Command Center, assuming each sensor observes averages less than 100 Mbps network traffic as throughput:

	Memory Requirements	Peak Sensor Throughput
≤20 Monitoring Sensors	16 GB	1 Gbps
≤30 Monitoring Sensors	32 GB	
≤40 Monitoring Sensors	48 GB	
≤50 Monitoring Sensors	64 GB	
≥50 Monitoring Sensors	80 GB	

### Migration from eyeSight Command Center to eyeInspect Command Center Guidance

It is important to understand that an eyeSight CC can be upgraded to an eyeInspect CC. The eyeInspect CC requires more resources, as it offers the complete eyeInspect capabilities, including threat detection and visualizations. However, the process of upgrading the VM from the eyeSight CC resource requirements to eyeInspect CC resource requirements is not trivial (e.g., disk resizing). For this reason, whenever possible it is recommended to align to the eyeInspect CC resource requirements from the start (see table in Section 2.1 above) to be future proof for later expansions.

## 3.0 Sensors

Sensors are an essential component of an OT deployment. Monitoring Sensors passively monitor and analyze network traffic from a group of hosts. The analysis of that traffic provides the richness of data visualized in the CC. Active Sensors selectively query devices using techniques specifically built or tuned for OT environments, to enrich device visibility and compliance verification.

### 3.1 Passive Monitoring Sensor Requirements

Monitoring Sensors should be installed on dedicated hardware – either rack servers or industrial PCs depending on the deployment location and type of monitored environment – or virtualized on VMware ESXi.

All Monitoring Sensors require at least two network interfaces. One network interface is used to connect to the Command Center. The other interfaces are used to monitor the traffic.

As general guidelines we suggest the following technical specifications:

	Small deployment (up to 250 Mbps)	Medium deployment (up to 500 Mbps)	Large deployment (1 Gbps and above)
Deployment description	Deployments in small networks and/or harsh environments	Deployments in medium sized networks and harsh environments	Deployments in large networks and data center installations
Hardware Form factor	Short-depth rack server or Small size industrial PC / DIN-rail fitting	19" 1U rack server or Medium size industrial PC	19" 1U rack server
Example hardware model	Supermicro SuperServer E300-9A-4CN10P	Axiomtek eBOX671-521-FL	Dell PowerEdge R640
Hypervisor	minimum VMware ESXi 5		
Processor	4-core (Intel) CPU 64 bits	4 or 6-core (Intel) CPU 64 bits with 8 GT/s	From 6-core (Intel) CPU 64 bits $\geq$ 2.4GHz with 8 GT/s
Memory size	8-16 GB	16-32 GB	64-256 GB
Memory type (physical deployment)	DDR4 2133MHz or better		
Hard drive	30 GB — 500 GB – In industrial PCs (wide-temperature) SSDs should be used.		
Network interface 1	Server management interface and connection to Command Center		
Network interface 2+	Monitoring interface(s)		

For virtualized deployments, the virtual network interface of the sensor may be attached to:

- A VMDirectPath I/O passthrough: this configuration is required when the traffic to be monitored enters the hypervisor from a physical network interface on the hypervisor server (for example, traffic mirrored from a physical network); this configuration bypasses the virtual switch and



requires a physical NIC to be exclusively dedicated to the virtual machine running the Monitoring Sensor.

- A virtual-only virtual switch (i.e., not attached to any physical network interface): this configuration is supported only when all monitored traffic originates within the hypervisor network, and no traffic comes from the physical network interfaces.

Details for the former configuration can be found on the [VMWare website](#).

### 3.2 Active Sensor Requirements

Active Sensors can be installed on dedicated hardware – either rack servers or industrial PCs depending on the deployment location and type of monitored environment – or virtualized on VMware ESXi.

The following are the minimum hardware requirements for Active Sensors; these requirements allow up to 50 concurrent active queries. Note that in case of bundled installations with Monitoring and Active Sensor on the same appliance, the Monitoring Sensor requirements indicated in the previous section will suffice to run both software components.

Processor	4-core (Intel) CPU 64 bits
Memory size	4 GB
Memory type (physical deployment)	Preferred DDR4-1866/2133
Hard drive	50 GB SSD
Network interface 1	Server management interface and connection to Command Center. The same interface can be used also to query network devices (if the traffic is routable to the devices being queried).
Network interface 2	Optional separate network interface used to query network devices.

## 4.0 Qualified Hardware Appliances

These models are certified and recommended by Forescout for use with eyeInspect software. **Please note that estimated lead-times on these appliances currently range from 12 to 16 weeks.**

### 4.1 Rack server — Dell® PowerEdge R640



- 1U rack server suitable for Command Center and Monitoring Sensors deployed in data centers
- High-performance and expandable
- Includes Dell® hardware warranty: Dell® ProSupport Next Business Day Onsite, 5 Years & Dell® ProSupport 7x24 Technical Support, 5 Years. More details: <https://www.dell.com/support/contents/us/en/04/category/warranty>.
- Gigabit Management Interface (built-in) and up to 12 network monitoring ports (Copper/Fiber)
- Dual, Hot-plug, Redundant Power Supply, 500-750W, Power input 100-240 VAC
- Max. Power Consumption 847.27W
- Max. Heat Dissipation 2891 BTU/hr
- Dell® iDRAC9 Enterprise included & Dell® ReadyRails™ sliding rail kit included

#### Monitoring Sensor Models for Dell PowerEdge R640

Monitoring Sensor for Monitoring up to 1 Gbps – 8 Network Monitoring Ports	
Forescout Part Number	SD-HW-S-FG1480 (Reference model)
Processor	2x Intel Xeon® Silver 4214 2.2G, 12C/24T CPU 64bit
Memory	32GB DDR4 3200MHz
Hard drive	480GB SSD
Management interface	1/10 GB Network card (Broadcom 57416 Dual Port 10GbE BASE-T & 5720 Dual Port 1GbE BASE) built-in
Monitoring interface (PCIe)	4 Copper, 2 Fiber, 2 unused SFP Ports (Copper – 1x Broadcom 5719 Quad 1Gbe, Fiber – 1x Silicom PE310G4I71L with 2 Finisar FTLX8574D3BCV 1G/10G 850nm Multimode Datacom SFP+ Transceivers supplied by Forescout)

Monitoring Sensor for Monitoring up to 1.6 Gbps – 12 Network Monitoring Ports	
Forescout Part Number	SD-HW-S-FG3960 (Reference model)
Processor	2x Intel Xeon® Gold 5218 2.3G, 16C/32T CPU 64bit
Memory	128GB DDR4 3200MHz
Hard drive	960GB SSD
Management interface	1/10 GB Network card (Broadcom 57416 Dual Port 10GbE BASE-T & 5720 Dual Port 1GbE BASE) built-in
Monitoring interface (PCIe)	8 Copper, 2 Fiber, 2 unused SFP Ports (Copper – 2x Broadcom 5719 Quad 1Gbe, Fiber – 1x Silicom PE310G4I71L with 2 Finisar FTLX8574D3BCV 1G/10G 850nm Multimode Datacom SFP+ Transceivers supplied by Forescout)

Monitoring Sensor for Monitoring up to 3.2 Gbps – 8 Network Monitoring Ports	
Forescout Part Number	SD-HW-S-FG8960 (Reference model)
Processor	2x Intel Xeon® Gold 6254 3.1G, 18C/36T CPU 64bit
Memory	256GB DDR4 3200MHz
Hard drive	960GB SSD (8 drives)
Management interface	10 GB Network card (QLogic FastLinQ 41162 Dual Port 10GbE BASE-T)
Monitoring interface (PCIe)	4 Copper, 4 Fiber (Copper - 1x Broadcom 5719 Quad Port 1GbE BASE-T, Fiber – 1x QLogic FastLinQ 41164 Quad Port 10GbE SFP+; Transceivers not included)

**Command Center Models for Dell PowerEdge R640**

Command Center – Up to 20 Sensors	
Forescout Part Number	SD-HW-CC-FG2960 (Reference model)
Processor	2x Intel Xeon® Gold 5218 2.3G, 16C/32T CPU 64bit
Memory	128GB DDR4 3200MHz
Hard drive	2x 960GB SSD
Management interface	1/10 GB Network card (Broadcom 57416 Dual Port 10GbE BASE-T & 5720 Dual Port 1GbE BASE) built-in

Command Center – Up to 100 Sensors	
Forescout Part Number	SD-HW-CC-FG8960 (Reference model)
Processor	2x Intel Xeon® Gold 6254 3.1G, 18C/36T CPU 64bit
Memory	256GB DDR4 3200MHz
Hard drive	4x 960GB SSD
Management interface	1/10 GB Network card (Broadcom 57416 Dual Port 10GbE BASE-T & 5720 Dual Port 1GbE BASE) built-in

## 4.2 Rack server — Forescout® 5120, 5140, 5160



- Suitable for Monitoring Sensors deployed in data centers.
- High-performance and expandable 1U rackmount.
- Forescout ActiveCare maintenance and support available. More details: <https://www.forescout.com/support-hub/customer-support/>.

Monitoring Sensor for Monitoring 1 Gbps to 3.2 Gbps	
Forescout Part Number	FS-HW-5120-OT, FS-HW-5140-OT, FS-HW-5160-OT <b>(expected availability Q4 2021)</b>
Sensor Throughput	FS 5120: up to 1 Gbps FS 5140: up to 1.4 Gbps FS 5160: up to 3.2 Gbps
Hard Drive	FS 5120, 5140: 3 HDD (RAID-1+HS) 600 GB FS 5160: 3 HDD (RAID-1+HS) 1.2 TB
Management Interface	1GB out of band management port
Copper Network Interfaces	4x 10/100/1000 Mbps Ethernet
SFP Network Interfaces	4x 1G/10G dual rate SR 2x Fiber SFPs included in base configuration
Power	Dual, Hot-plug, Redundant Power Supply, 750W – 100-240VAC Max power consumption: 847.27W
Operating Temperature	10°C to 35°C (50°F to 95°F)
Max. Heat Dissipation	2891 BTU/hr

### 4.3 Short-depth rack server — Supermicro SuperServer E300-9A-4CN10P



- Suitable for Monitoring Sensors deployed in small networks or networks with limited throughput (up to 300Mbps); not suitable for running both passive and active sensor.
- Short-depth, 1U rack mountable (mounting kit included)
- IPMI OOB management (Out-Of-Band Intelligent Platform Management Interface)
- Manufacturer’s warranty: 3 Years labor, 1 Year Parts, 1 Year Cross-ship. More details: <https://www.supermicro.com/en/support/warranty>

Monitoring Sensor for Monitoring up to 300 Mbps	
Forescout Part Number	SD-HW-S-SME300 (Reference model; SMC PN: SYS-E300-9A4C10P-1-FT026)
Processor	Intel® Atom® processor C3558, 2.2G, 4C/4T, CPU 64bit
Memory	8GB DDR4 2133MHz DIMM
Hard drive	240GB Solid State Drive
Management interface	1 GB Network card (Marvell® Alaska® 88E1543)
Monitoring interface (PCIe)	4 Copper (Intel® I350), 2 Fiber (Intel® I210)
Power	84W AC/DC power adapter included Max power consumption: 41W
Dimensions	254 mm wide x 43 mm high x 226 mm deep
Mounting Options	Rackmount kit included (MCP-290-30002-0B)
Max. Heat Dissipation	139.90 BTU/hr
Certifications	CE/FCC/UL/CB/BSMI/VCCI

### 4.4 Industrial PC — Forescout® 4130



- Recommended option for Monitoring Sensors deployed in harsh environments.
- Powerful and fanless industrial box PC with wide-range operating temperature and power input.
- Forescout ActiveCare maintenance and support available. More details: <https://www.forescout.com/support-hub/customer-support/>.

Monitoring Sensor for Monitoring up to 600 Mbps	
Forescout Part Number	FS-HW-4130-OT
Processor	Gen 8 Intel® Core™ i5-8500T, 6C/6T CPU 64bit
Memory	32GB (2x16G) 2666MHz DDR4 SO-DIMM
Hard drive	512GB Solid State Drive SATA III
Management interface (built-in)	2 x 10/100/1000 Mbps Ethernet (i210-IT & i219-LM)
Monitoring interface (PCIe)	4 x 10/100/1000 Mbps Ethernet (i210-IT)
Power	Nominal input 24VDC. Power Supply: 100-240 VAC, up to 120W, 50-60Hz (AC/DC adapter included) Max power consumption: 52.8W
Dimensions	280 mm wide x 210 mm deep x 80.5 mm high 4.8 kg (10.58 lb)
Mounting Options	Wall mount (part number 8816K6718A0E) included, DIN Rail kit (8816K6719A0E) available for purchase at: <a href="https://www.arrow.com/en/campaigns/forescout">https://www.arrow.com/en/campaigns/forescout</a>
Operating Temperature	-40°C to +50°C
Max Heat Dissipation	180.16 BTU/hr
Certifications	CE, FCC Class A, IP40, IEC 60068

### 4.5 Industrial PC — Schweitzer Engineering Laboratories® SEL-3350



- Suitable for Monitoring Sensors deployed in electric power substations.
- Fanless industrial box PC with wide-range operating temperature and power input.
- Substation IEEE 1613 Compliant
- SEL 10-Year Product Warranty. More details: <https://selinc.com/company/quality/>

Monitoring Sensor for Monitoring up to 180 Mbps	
Forescout Part Number	SD-HW-S-SEL3350 (Reference model; <b>expected availability Q4 2021</b> )
Processor	Intel Atom x5-E3940, 4C/4T Frequency: 1.6 GHz Cache: 2 MB L2
Memory	8 GB DDR3L ECC PC3-1600 (800 MHz)
Hard drive	120GB industrial multilevel cell (iMLC) SSD
Management interface (built-in)	1x 10/100/1000 Mbps Ethernet
Monitoring interface (PCIe)	4x 10/100/1000 Mbps Ethernet
Power	High voltage power supply 48–125 VDC or 110–120 VAC
Dimensions	1U 19" rack-mount chassis; 1U rack-mount panel included
Operating Temperature	–40°C to +85°C
Certifications	IEEE 1613, IEEE C37.90, IEC 61850-3, IEC 60255 protective relay standards IEC 61000-6-2 and IEC 61000-6-4 industrial environment standards



### 4.6 Industrial PC — Schweitzer Engineering Laboratories® SEL-3355



- Suitable for Monitoring Sensors deployed in electric power substations.
- Powerful and fanless industrial box PC with wide-range operating temperature and power input.
- Substation IEEE 1613 Compliant
- SEL 10-Year Product Warranty + 5 years on NIC installed by Foxguard. More details: <https://selinc.com/company/quality/>

Monitoring Sensor for Monitoring up to 500 Mbps	
Forescout Part Number	SD-HW-S-SL1480 (Reference model)
Processor	Intel Xeon® E3-1505L 2.0G, 4C/8T CPU 64bit
Memory	16GB (1x16G) DDR4 2133MHz memory
Hard drive	480GB industrial multilevel cell (iMLC) SSD
Management interface (built-in)	Two 10/100/1000 Mbps Ethernet port connections on the rear panel support high-speed network connectivity and enable connections to independent networks or redundant paired network connections.
Monitoring interface (PCIe)	8x 10/100/1000 Mbps Ethernet (2x Intel i350)
Power	Single 160W High Voltage power supply included that supports either 125/250VDC or 120/220/240VAC. This appliance allows for a second power supply to be installed (not available through Forescout). This second power supply could be either an identical model as mentioned above, or a 48VDC 160W Low Voltage model. Max. power consumption: 91.94W
Dimensions	3U 19" rack-mount chassis; 3U rack-mount panel included
Operating Temperature	-40°C to +60°C
Max. Heat Dissipation	313.72 BTU/hr
Certifications	IEEE 1613-2009 plus many other IEC, IEEE, FCC and CISPR – available upon request.

### 4.6 DIN-Rail industrial PC — FoxGuard® Solutions IADIN-FS1



- Suitable for Monitoring Sensors deployed in harsh environments.
- No moving parts (fanless), wide-range temperature range and offers DIN-rail mounting.

Monitoring Sensor for Monitoring up to 400 Mbps	
Forescout Part Number	SD-HW-S-FG1250 (Reference model)
Processor	Intel i5-7x00U 2.5G, 2C/4T CPU 64bit
Memory	16GB (2x8G) DDR4 2133MHz memory
Hard drive	250GB SSD
Management interface (built-in)	Intel Gigabit LAN
Monitoring interface (PCIe)	4x 10/100/1000 copper (1x Intel i350)
Power	12VDC (locking barrel connector) - 60W AC/DC adapter included
Dimensions	142 x 185 x 60mm (DxWxH)
Mounting Options	Wall mount and DIN-rail mount included
Operating Temperature	0 to 40* C
Max Heat Dissipation	30.3 BTU/hr

Forescout Technologies, Inc. 190 West Tasman Drive San Jose, CA 95134 USA

**Toll-Free (US)** 1-866-377-8771  
**Tel (Intl)** +1-408-213-3191  
**Support** 1-708-237-6591

© 2021 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 8/21**