FORESCOUT

Name: ____________________________________

The Forescout Test Drive

Experience the Difference of Agentless Device Visibility and Control

V 1.0

Contents

Introduction

Forescout Test Drive demos let you experience the powerful features of the Forescout platform firsthand. They provide you with a live Forescout instance in a virtual lab environment and easy-to-follow, step-by-step guidance for exploring the product. **No Forescout experience necessary**.

Following a quick introduction, today's course will take you through four real-world scenarios:

- **Lap One: Visibility.** You can't secure what you can't see.™ Learn how to discover every physical and virtual device connected to your network, classify them, and assess their security posture.
- **Lap Two: Asset Management.** Agentless device visibility and continuous monitoring fuel every aspect of cybersecurity. Access a real-time hardware and software asset inventory for an annual software audit—without pulling resources from other critical tasks. Query the Asset Inventory to quickly obtain valuable device-related information.
- **Lap Three: Incident Response.** Put the Forescout policy engine through its paces as you respond to a WannaCry outbreak. Use an automated policy to quickly locate vulnerable hosts and determine which need to be patched and which are infected—instead of the complex process most enterprises use today. Create dashboard entries so you can monitor your progress while responding to this incident.
- **Lap Four: Network Segmentation** Assess the devices on your network and make sure they can only access the resources they need. Segment access based on device type and security posture to reduce the risks posed by rogue and noncompliant devices.

Scenario

You are the Chief Information Security Officer of a small company, ThingCo, that distributes Things. Your growing company recently moved into a larger facility that has a distribution center attached to it. The automated systems in the distribution center can be controlled from the corporate network.

You recently discovered that contractors plugged a consumer wireless access point into the distribution center network to make it easier for them to get their systems on the network, and then left it there. The device is not secured. Luckily, there was no sign of a breach, and its presence did not affect the older industrial control systems running on that network.

However, it highlighted an issue that you have been trying to address. Your company's quarterly e-mail asking about the devices people have on the network, and the manual collection and entry of that information, are clearly not sufficient. Additionally, the agent-based audits of software running on your network are missing many devices in your environment that cannot have agents installed on them. You need a real-time, agentless view into your network.

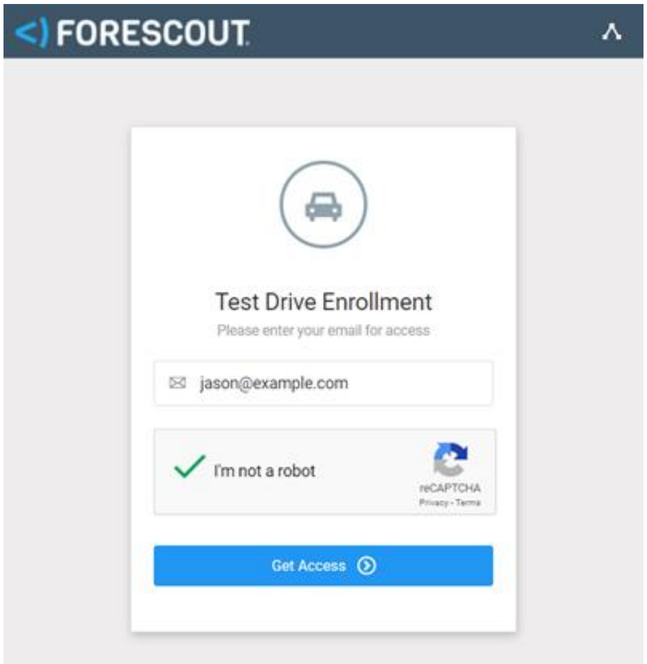
After hearing about the capabilities of the Forescout platform, you decided to bring it in for a Proof of Value on your network.

Warm-Up Lap: Starting the Demo Environment

The Test Drive uses virtual devices in a cloud-based environment accessed through your web browser to give you a hands-on experience with the Forescout platform. Before the session begins, you need to enable your lab.

Step 1: Open your web browser and point it to https://demoit.online/testdrive.

Note: Google Chrome is the recommended web browser.



Test Drive Enrollment

Please enter your email for access

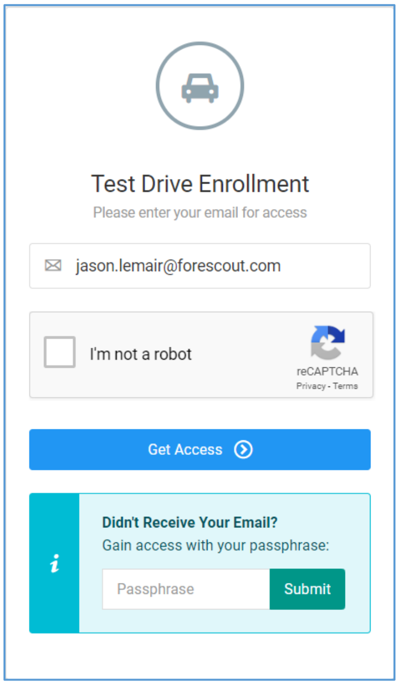
jason@example.com

☑ I'm not a robot

Step 2: Enter your e-mail address you used to register for the course and check the I'm not a robot checkbox. Click **Get Access**.

You will receive an email address with the link to your lab.

IMPORTANT: If you do not have access to your email, or you do not receive the message within a few minutes, ask the session moderator for the lab passphrase and enter it in the **Didn't Receive Your Email?** Field on the login page.



Test Drive Enrollment

Please enter your email for access

jason.lemair@forescout.com

□ I'm not a robot

Get Access

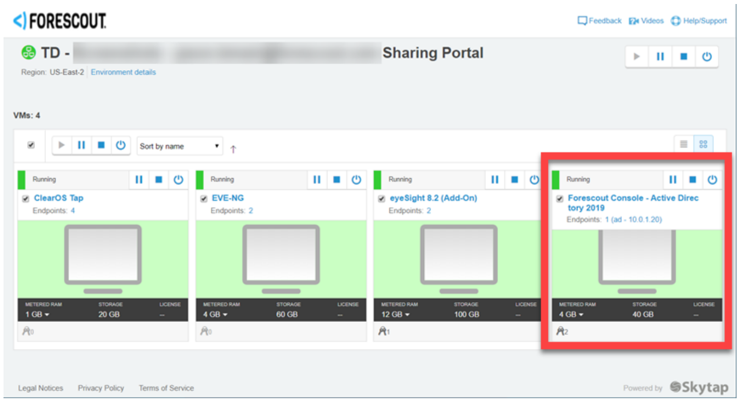
Didn't Receive Your Email?

Gain access with your passphrase:

Passphrase | Submit

Step 3: Click the link in your email message.

Your lab console with three devices appears.



TD - [redacted] Sharing Portal

Region: US-East-2 | Environment details

VMs: 4

Sort by name

Running	Running	Running	Running
ClearOS Tap	EVE-NG	eyeSight 8.2 (Add-On)	Forescout Console - Active Directory 2019
Endpoints: 4	Endpoints: 2	Endpoints: 2	Endpoints: 1 (ad - 10.0.1.20)
METERED RAM 1 GB STORAGE 20 GB LICENSE –	METERED RAM 4 GB STORAGE 60 GB LICENSE –	METERED RAM 12 GB STORAGE 100 GB LICENSE –	METERED RAM 4 GB STORAGE 40 GB LICENSE –
0	0	1	2

Step 4: Minimize your browser. You will be instructed when to access the lab devices shortly.

FORESCOUT

Lap 1: Visibility

Scenario

You heard that a recent study conducted by IDC found that Forescout customers see 24% more devices than expected on their networks—some seeing as high as 60% more. You had some doubts about the numbers, so you decided to try the Forescout platform on your own network.

After installing the Forescout platform, you discovered that there were many more devices attached to network than you anticipated—lab computers connected to the corporate network, consumer wireless access points that were not part of the planned infrastructure, non-corporate mobile devices, many more network-connected smart speakers than you expected—even a game console and a smart TV.

Forescout has pioneered an agentless approach to security that provides real-time discovery, classification, assessment and monitoring of devices, allowing you to see what's on your network, from campus to cloud, and to securely manage it.

Before you begin

- How do you currently track the devices that connect to your network? How many devices do you currently have on your network? How confident are you that the number is accurate?
- Why types of devices are they? How do you know?

In this lap, you will:

1. Learn about how the Forescout platform discovers, classifies, and assesses the devices on your network.
2. Access your lab environment.
3. Use the Dashboard to View the Devices on Your Network
4. Use the Dashboard to Check Your Endpoint Compliance

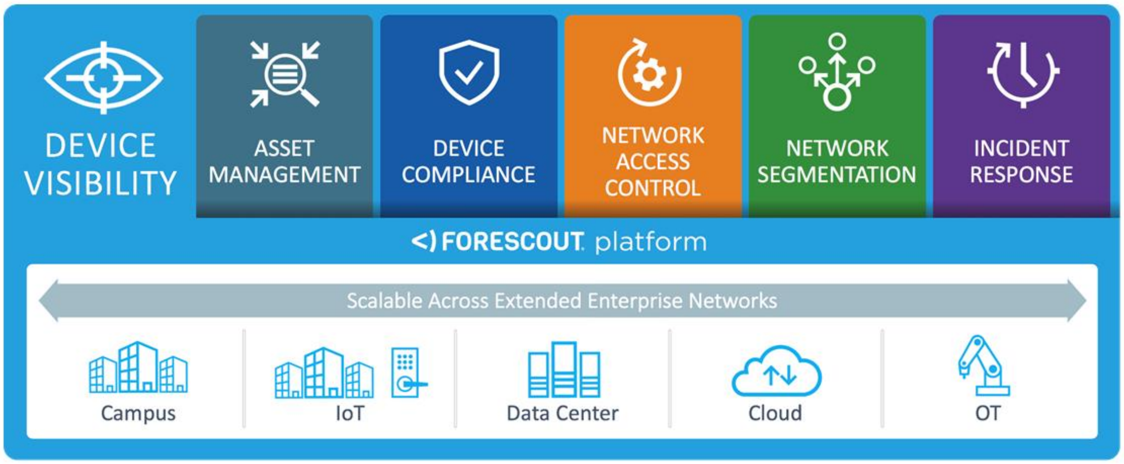
Task 1: How Does Forescout See Devices?

Follow along with the Test Drive leaders as they guide you through how the Forescout platform gives you visibility into the devices on your network.

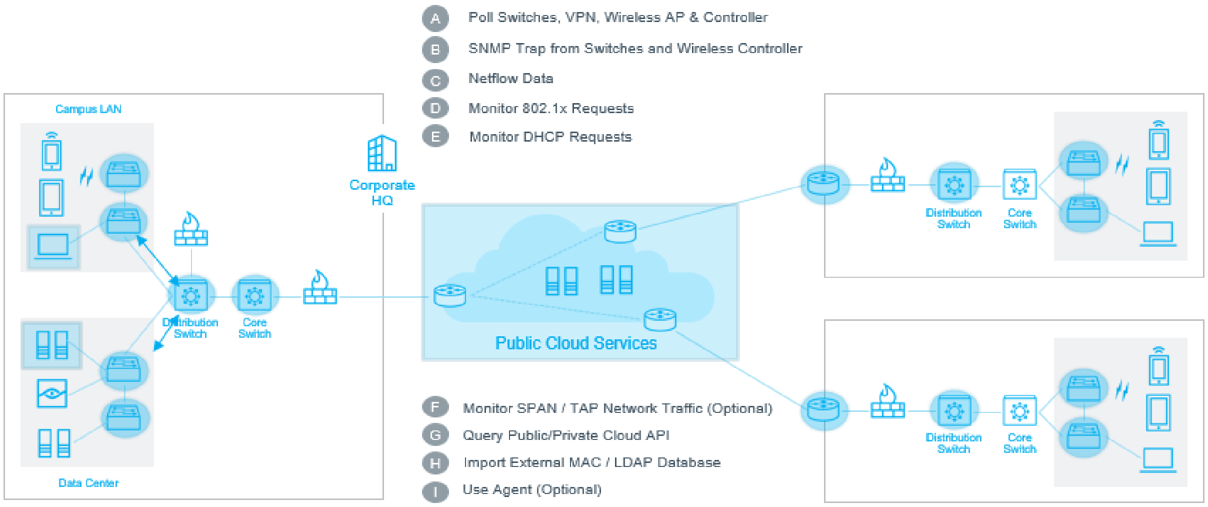
The foundation of the Forescout platform is visibility. This need for visibility goes across the entire enterprise—campus, IoT, data center, cloud and operational technology (OT) environments—and comes together to solve a variety of use cases that address your business needs:

- Asset Management
- Device Compliance
- Network Access Control
- Network Segmentation
- Incident Response

Forescout's Mission: 100% Device Visibility and Control



Using a combination of active and passive monitoring techniques, Forescout eyeSight provides in-depth visibility to discover devices the instant they enter the network—without requiring agents. eyeSight classifies and assesses these devices and virtual instances, then continuously monitors them as they come and go from the network.


A Poll Switches, VPN, Wireless AP & Controller
B SNMP Trap from Switches and Wireless Controller
C Netflow Data
D Monitor 802.1x Requests
E Monitor DHCP Requests
Campus LAN
Corporate HQ
Distribution Switch
Core Switch
Public Cloud Services
Data Center
F Monitor SPAN / TAP Network Traffic (Optional)
G Query Public/Private Cloud API
H Import External MAC / LDAP Database
I Use Agent (Optional)

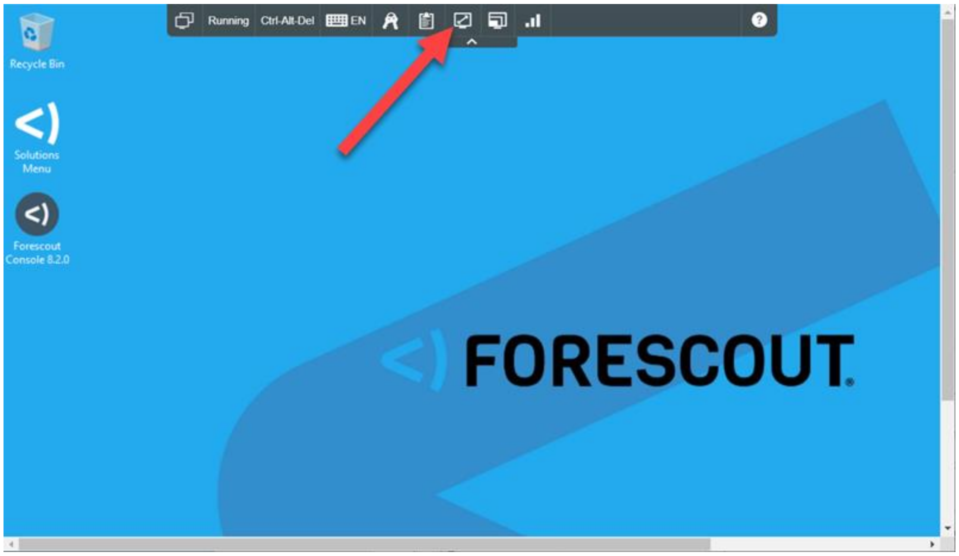
Task 2: Access Your Lab

You can see the devices on your network using the Forescout platform’s dashboard.

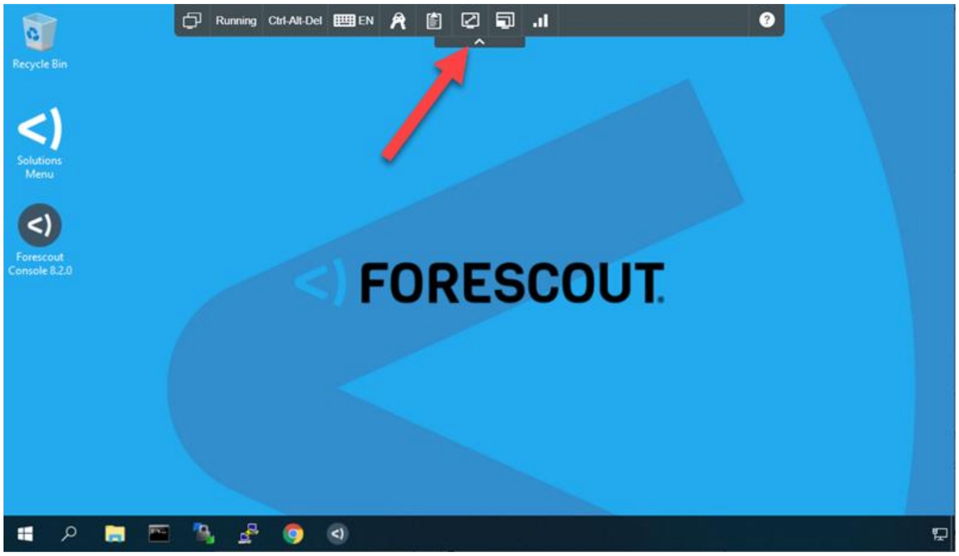
Step 1: Switch to the web browser that you logged into the lab with and make the browser full screen.

Step 2: Click the **Forescout Console – Active Directory 2019** device.

The device interface (Windows) opens in a new tab.



Step 3: Click the **Fit to Window** icon in the toolbar at the top.



Step 4: Click the **Toggle Toolbar** button to move the toolbar out of the way.

Task 3: Use the Dashboard to View the Devices on Your Network

The Forescout platform's default dashboards provide an easy way to view the devices that eyeSight discovers on your network and the states of those devices.

Step 1: Click the Chrome icon in the taskbar at the bottom of the screen.

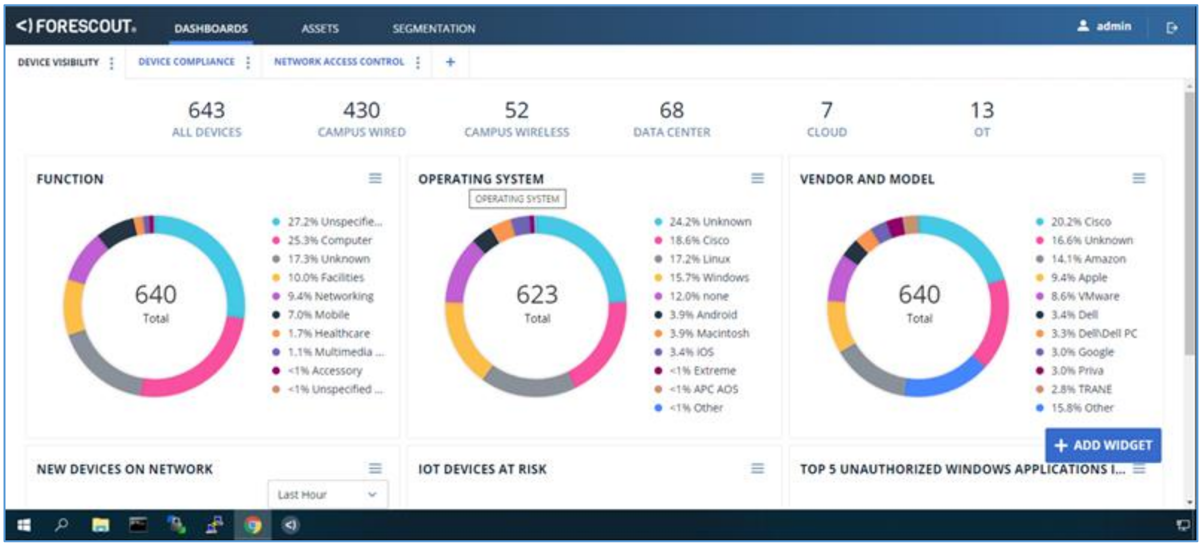
Step 2: Click the **eyeSight Dashboard** entry in the browser bookmark bar.

The dashboard login screen appears

Step 3: Log in using the pre-populated credentials. The login credentials should be pre-populated. If they are not, use:

User Name: admin
Password: 4Scout123

The first dashboard you see is the Device Visibility dashboard. Across the top is a summary of the devices eyeSight discovered on your network by type of device (Campus Wired, Campus Wireless, Data Center, Cloud, and OT)

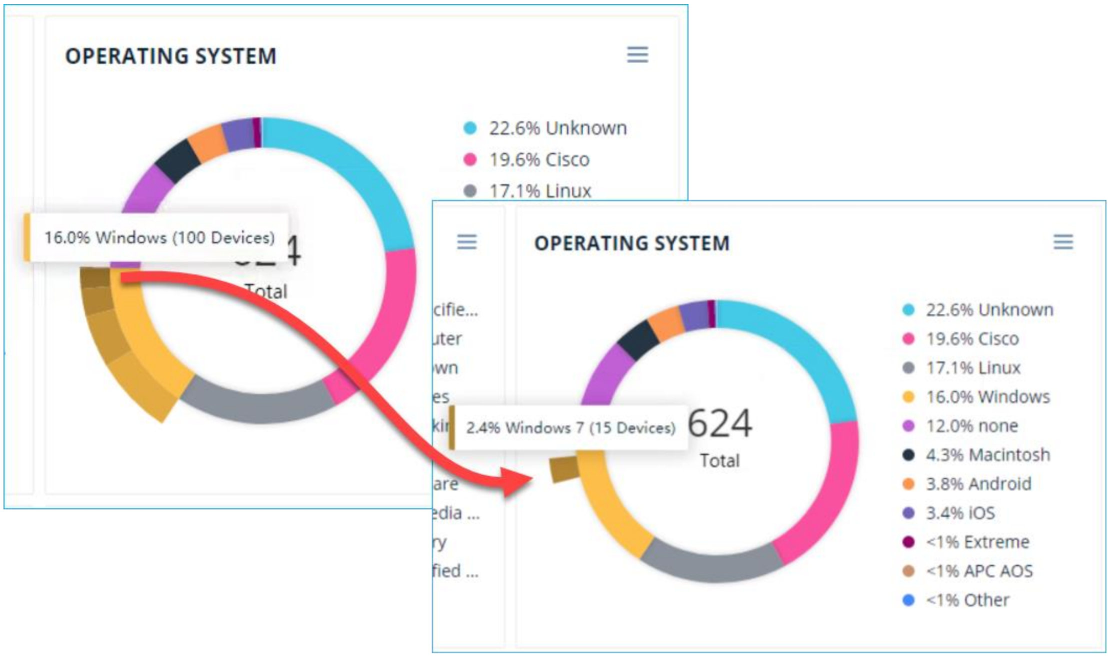


Below the summary are the following 6 Widgets that provide various views of the devices on your network:

- **Function**—is it a mobile device, medical device, computer?
- **Operating System**—what OS is it running?
- **Vendor and Model**—who made the device?
- **New Devices on Network**—how many devices have come on the network in the past hour, day, week, month, or year?
- **IOT Devices at Risk**—which IoT devices are have weak or default credentials or insecure ports open?
- **Top 5 Unauthorized Windows Applications Installed**—which applications that violate your company policies do users have installed on their endpoints?

Step 4: Hover your cursor over the Windows entry in the Operating System chart.

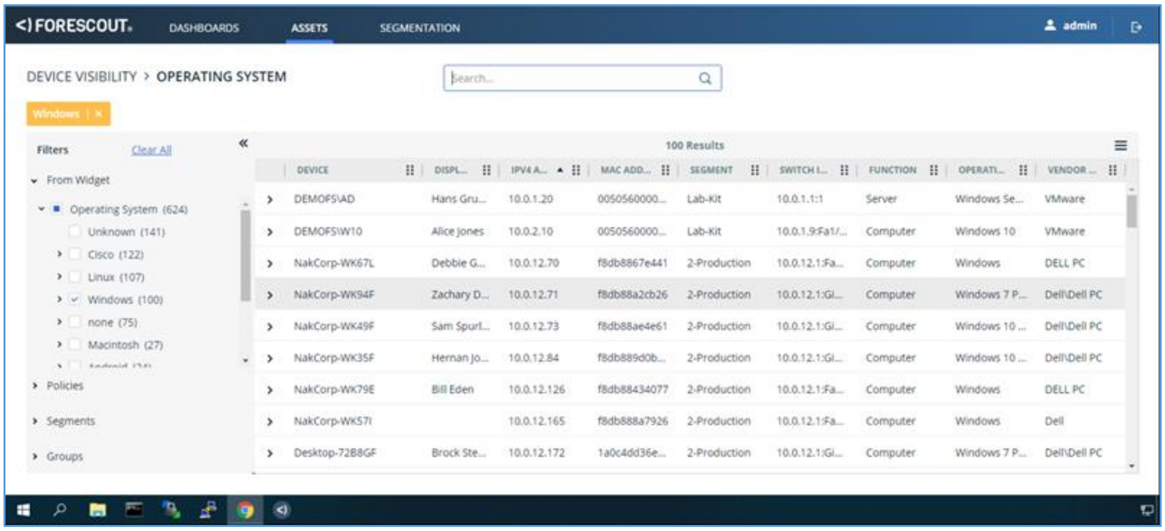
That part of the ring diagram expands to show additional information. In this case, it breaks down the Windows devices by Windows version.



NOTE: Your diagrams will have different data from the ones above.

Step 5: Click the Windows part of the Operating System diagram.

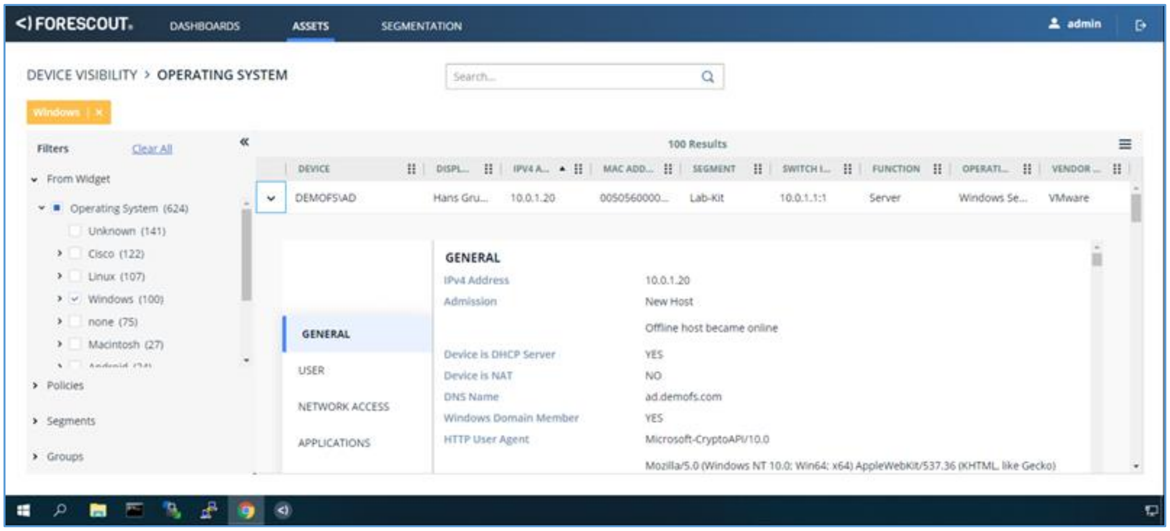
Dashboard displays the list of Windows devices.



100 Results

	DEVICE	DISPL...	IPV4 A...	MAC ADD...	SEGMENT	SWITCH I...	FUNCTION	OPERATI...	VENDOR ...
›	DEMOFS\AD	Hans Gru...	10.0.1.20	0050560000...	Lab-Kit	10.0.1.1:1	Server	Windows Se...	VMware
›	DEMOFS\W10	Alice Jones	10.0.2.10	0050560000...	Lab-Kit	10.0.1.9:Fa1/...	Computer	Windows 10	VMware
›	NakCorp-WK67L	Debbie G...	10.0.12.70	f8db8867e441	2-Production	10.0.12.1:Fa...	Computer	Windows	DELL PC
›	NakCorp-WK94F	Zachary D...	10.0.12.71	f8db88a2cb26	2-Production	10.0.12.1:Gi...	Computer	Windows 7 P...	Dell\Dell PC
›	NakCorp-WK49F	Sam Spurl...	10.0.12.73	f8db88ae4e61	2-Production	10.0.12.1:Gi...	Computer	Windows 10 ...	Dell\Dell PC
›	NakCorp-WK35F	Hernan Jo...	10.0.12.84	f8db889d0b...	2-Production	10.0.12.1:Gi...	Computer	Windows 10 ...	Dell\Dell PC
›	NakCorp-WK79E	Bill Eden	10.0.12.126	f8db88434077	2-Production	10.0.12.1:Fa...	Computer	Windows	DELL PC
›	NakCorp-WK57I		10.0.12.165	f8db888a7926	2-Production	10.0.12.1:Fa...	Computer	Windows	Dell
›	Desktop-72B8GF	Brock Ste...	10.0.12.172	1a0c4dd36e...	2-Production	10.0.12.1:Gi...	Computer	Windows 7 P...	Dell\Dell PC

Step 6: Click the carat to the left of the device to reveal detailed information about that device.



DEVICE VISIBILITY > OPERATING SYSTEM

100 Results

DEVICE	DISPL...	IPV4 A...	MAC ADD...	SEGMENT	SWITCH I...	FUNCTION	OPERATI...	VENDOR ...
DEMOFS\AD	Hans Gru...	10.0.1.20	0050560000...	Lab-Kit	10.0.1.1:1	Server	Windows Se...	VMware

GENERAL

IPv4 Address	10.0.1.20
Admission	New Host
	Offline host became online
Device is DHCP Server	YES
Device is NAT	NO
DNS Name	ad.demofs.com
Windows Domain Member	YES
HTTP User Agent	Microsoft-CryptoAPI/10.0
	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

You can use the filters on the left to filter the display based on policy, segment, and group.

Step 7: Click **Device Visibility** at the top of the screen to go back to the dashboard. Take a moment to explore the data in the other widgets on the dashboard. Return to the dashboard when done.

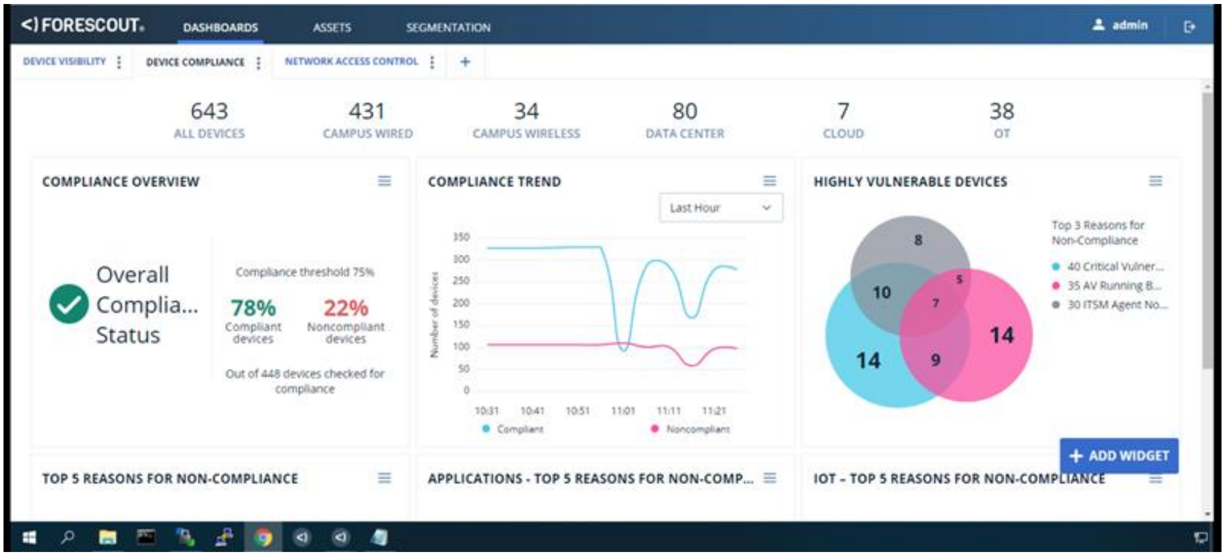
Task 4: Use the Dashboard to Check Your Endpoint Compliance

You can also quickly check on the compliance status of the devices on your network, such as having antivirus running and up to date or having disk encryption enabled.

Step 1: Click the Device Compliance tab at the top of the dashboard.

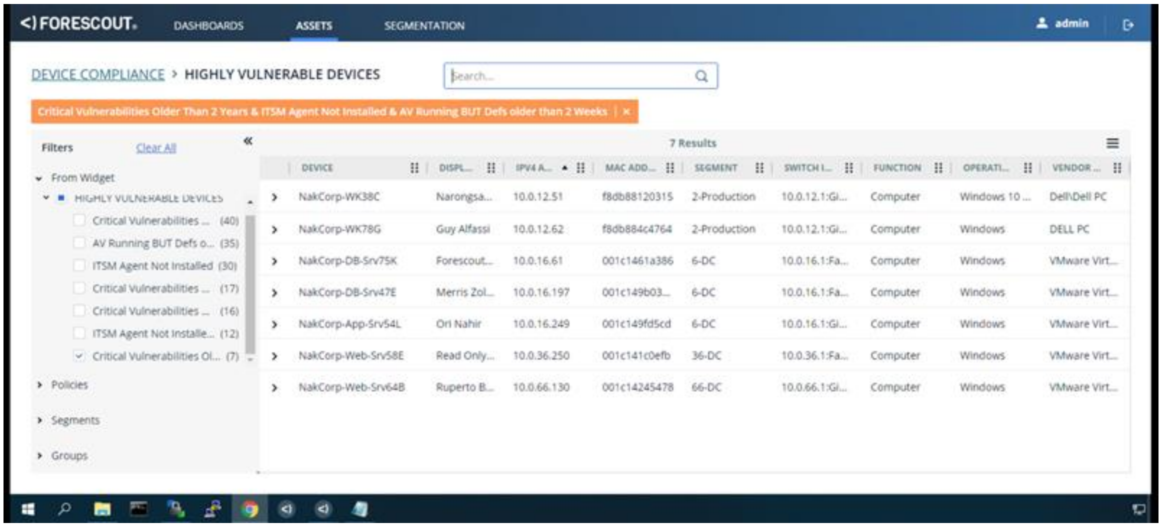
The Device Compliance Dashboard contains the following information:

- **Compliance Overview**—overall, what percentage of the devices on your network are compliant with your company policies?
- **Compliance Trend**—view the trend of compliant vs noncompliant devices on your network over time.
- **Highly Vulnerable Devices**—presents a VENN diagram of the top 3 reasons that devices are noncompliant. The intersection of those three reasons show you the most vulnerable devices on your network.
- **Top 5 Reasons for Non-Compliance**—the top 5 reasons that devices were marked noncompliant
- **Applications – Top 5 Reasons for Non-Compliance**—the top 5 reasons due to applications (out of date, not running, installed but not permitted) that devices were marked non-compliant.
- **IOT – Top 5 Reasons for Non-Compliance**—The top 5 reasons your IOT devices, such as printers, IP cameras, etc. were marked as noncompliant.



Step 2: In the **Highly Vulnerable Devices** widget, click the intersection of the three circles.

This widget shows the top three reasons for devices that are out of compliance. The intersection of the circles shows the most vulnerable devices – those with all three noncompliance attributes.



Critical Vulnerabilities Older Than 2 Years & ITSM Agent Not Installed & AV Running BUT Defs older than 2 Weeks | ×

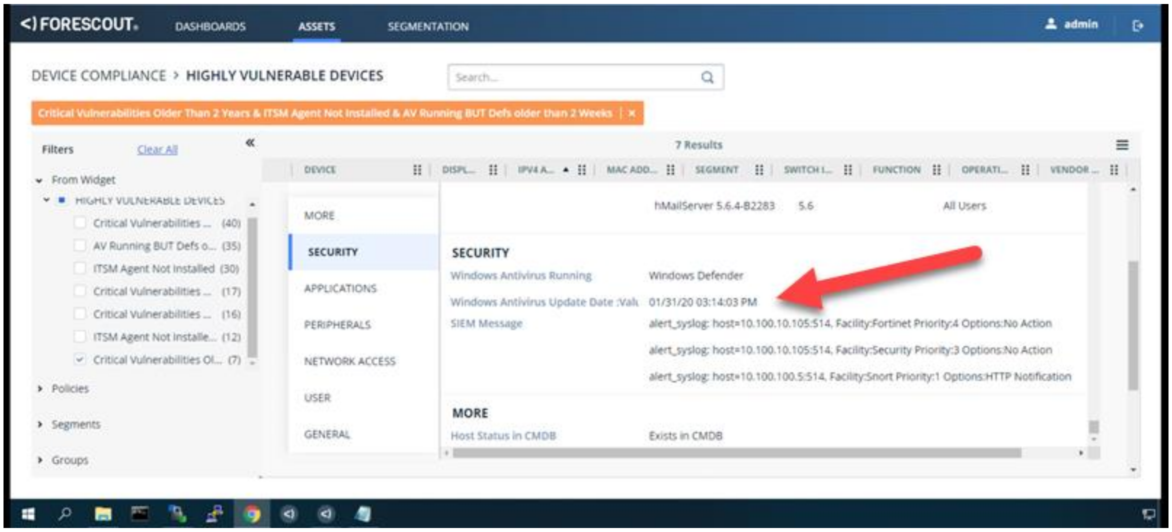
HIGHLY VULNERABLE DEVICES
- □ Critical Vulnerabilities ... (40)
- □ AV Running BUT Defs o... (35)
- □ ITSM Agent Not Installed (30)
- □ Critical Vulnerabilities ... (17)
- □ Critical Vulnerabilities ... (16)
- □ ITSM Agent Not Installe... (12)
- ☑ Critical Vulnerabilities Ol... (7)

7 Results

	DEVICE	DISPL...	IPV4 A... ▲	MAC ADD...	SEGMENT	SWITCH I...	FUNCTION	OPERATI...	VENDOR ...
›	NakCorp-WK38C	Narongsa...	10.0.12.51	f8db88120315	2-Production	10.0.12.1:Gi...	Computer	Windows 10 ...	Dell\Dell PC
›	NakCorp-WK78G	Guy Alfassi	10.0.12.62	f8db884c4764	2-Production	10.0.12.1:Gi...	Computer	Windows	DELL PC
›	NakCorp-DB-Srv75K	Forescout...	10.0.16.61	001c1461a386	6-DC	10.0.16.1:Fa...	Computer	Windows	VMware Virt...
›	NakCorp-DB-Srv47E	Merris Zol...	10.0.16.197	001c149b03...	6-DC	10.0.16.1:Fa...	Computer	Windows	VMware Virt...
›	NakCorp-App-Srv54L	Ori Nahir	10.0.16.249	001c149fd5cd	6-DC	10.0.16.1:Gi...	Computer	Windows	VMware Virt...
›	NakCorp-Web-Srv58E	Read Only...	10.0.36.250	001c141c0efb	36-DC	10.0.36.1:Fa...	Computer	Windows	VMware Virt...
›	NakCorp-Web-Srv64B	Ruperto B...	10.0.66.130	001c14245478	66-DC	10.0.66.1:Gi...	Computer	Windows	VMware Virt...

Step 3: Click the caret to the left of one of the devices, and then click **Security** in the device details.

The device details show when the last time the virus definition files was updated.


<) FORESCOUT.
DASHBOARDS
ASSETS
SEGMENTATION
admin
DEVICE COMPLIANCE > HIGHLY VULNERABLE DEVICES
Search...
Filters
Clear All
From Widget
HIGHLY VULNERABLE DEVICES
Critical Vulnerabilities ... (40)
AV Running BUT Defs o... (35)
ITSM Agent Not Installed (30)
Critical Vulnerabilities ... (17)
Critical Vulnerabilities ... (16)
ITSM Agent Not Installe... (12)
Critical Vulnerabilities Ol... (7)
Policies
Segments
Groups
7 Results
DEVICE
DISPL...
IPV4 A...
MAC ADD...
SEGMENT
SWITCH I...
FUNCTION
OPERATI...
VENDOR ...
MORE
SECURITY
APPLICATIONS
PERIPHERALS
NETWORK ACCESS
USER
GENERAL

Critical Vulnerabilities Older Than 2 Years & ITSM Agent Not Installed & AV Running BUT Defs older than 2 Weeks | ×

hMailServer 5.6.4-B2283 5.6 All Users

SECURITY

Windows Antivirus Running	Windows Defender
Windows Antivirus Update Date :Valı	01/31/20 03:14:03 PM
SIEM Message	alert_syslog: host=10.100.10.105:514, Facility:Fortinet Priority:4 Options:No Action alert_syslog: host=10.100.10.105:514, Facility:Security Priority:3 Options:No Action alert_syslog: host=10.100.100.5:514, Facility:Snort Priority:1 Options:HTTP Notification

MORE

Host Status in CMDB	Exists in CMDB

Step 4: Click **Device Compliance** at the top of the screen to go back to the dashboard. Take a moment to explore the data in the other widgets on the dashboard. Return to the dashboard when done.

Lap 2: Asset Management

Scenario

After the incident with the unsecured wireless access point, your company has decided that it needs to improve their asset management policies and procedures. Management wants tighter control of the hardware and software running on the network.

Because you are already trying the Forescout platform, you have decided to use it to gain visibility of the hardware and software on your network without pulling resources from other critical tasks.

The Forescout platform enables you to discover every Internet Protocol (IP) addressable device that connects to your network, in real time. Using both agentless and agent-based technology, it shows you the software and processes running on the managed endpoints on your network. The Forescout platform can provide detailed visibility into the devices in your operational technology environments.

Once you discover the devices, the Forescout platform classifies them using several criteria: type and function, operating system (OS) and version, manufacturer, model, and network function. Finally, Forescout can assess whether the devices are corporate-managed devices, and if those managed devices comply with corporate policy.

Before you begin

- How do you currently track hardware and software assets in your organization? Spreadsheets? Dedicated applications? Configuration management database (CMDB)?
- How do you keep it current? Surveys? Real-time data collection?
- How confident are you that your asset management tool is up to date with today's information?
- Who are the consumers of this data? How are they using it? What is the impact of inaccurate, out-of-date, or incomplete data to these users?

In this lap, you will:

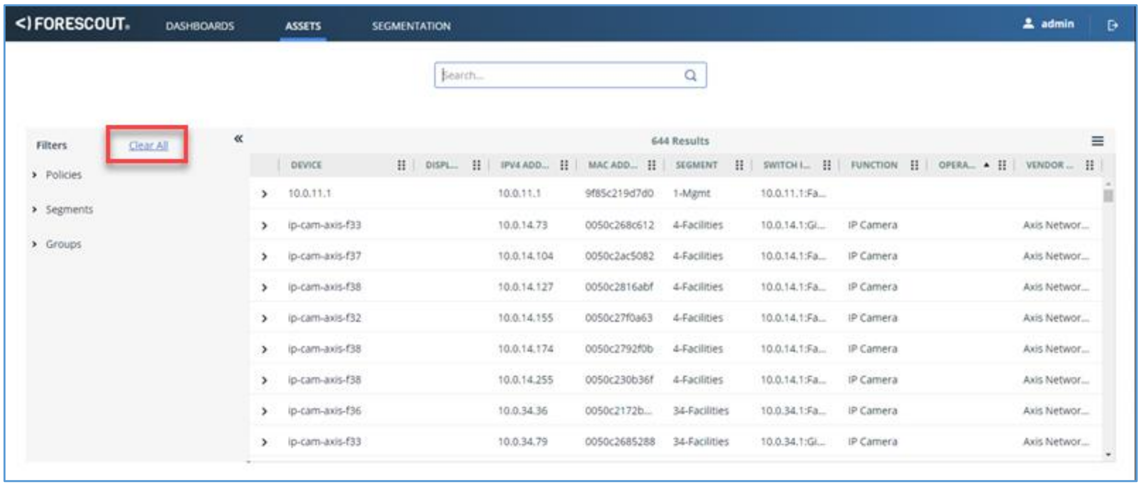
1. Use the Assets dashboard to see devices and operating systems on your network.
2. Log into the Forescout console.
3. Use the Asset Inventory to quickly see how many endpoints are running Microsoft Office (and which versions).
4. Use the Asset Inventory to see the operational technology devices running in your distribution center.
5. Use the Forescout Home tab to see all the devices running in your distribution center—both OT and IT devices.

Task 1: Discover the Versions of Windows on Your Windows Desktop Endpoints

You can use the Assets tab to view the devices on your network. You might have noticed that you already used this tab—each time you drilled down in the device dashboards, you were viewing the devices on the Assets tab.

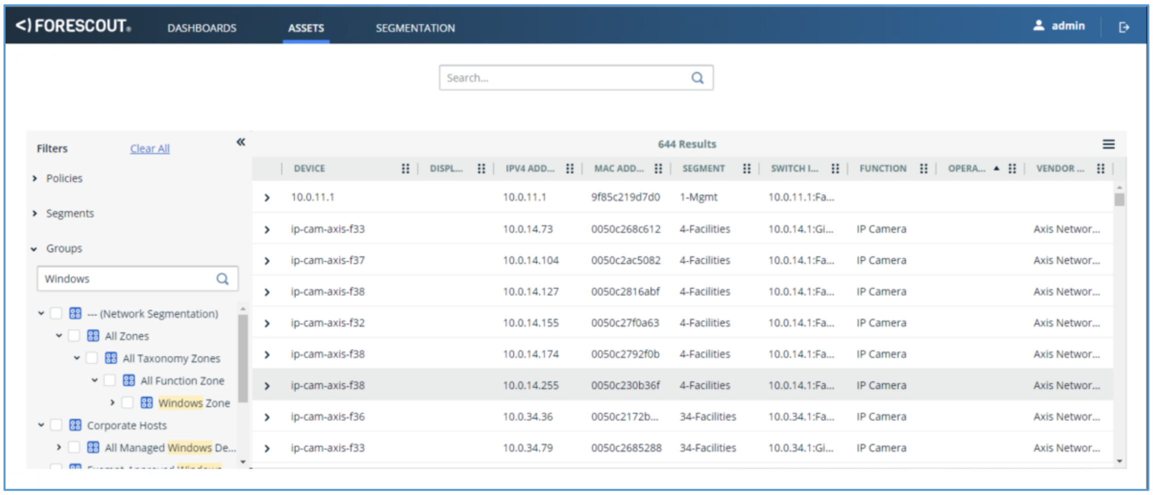
You want to see what versions of Windows are running on your end users' desktops. You suspect there may be several out-of-support versions still in use, which could introduce vulnerabilities on your network.

Step 1: Click the **Assets** tab at the top of the screen. If there is a filter applied to the view, click **Clear All**.



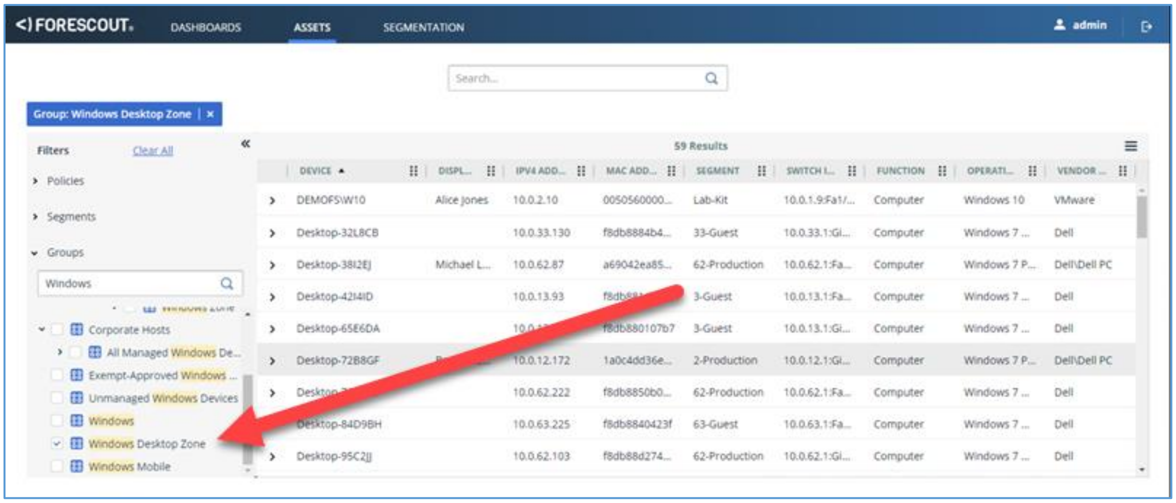
	DEVICE	DISPL...	IPV4 ADD...	MAC ADD...	SEGMENT	SWITCH I...	FUNCTION	OPERA... ▲	VENDOR ...
›	10.0.11.1		10.0.11.1	9f85c219d7d0	1-Mgmt	10.0.11.1:Fa...			
›	ip-cam-axis-f33		10.0.14.73	0050c268c612	4-Facilities	10.0.14.1:Gi...	IP Camera		Axis Networ...
›	ip-cam-axis-f37		10.0.14.104	0050c2ac5082	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f38		10.0.14.127	0050c2816abf	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f32		10.0.14.155	0050c27f0a63	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f38		10.0.14.174	0050c2792f0b	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f38		10.0.14.255	0050c230b36f	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f36		10.0.34.36	0050c2172b...	34-Facilities	10.0.34.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f33		10.0.34.79	0050c2685288	34-Facilities	10.0.34.1:Gi...	IP Camera		Axis Networ...

Step 2: Expand the **Groups** filter. Type **Windows** in the search field.



	DEVICE	DISPL...	IPV4 ADD...	MAC ADD...	SEGMENT	SWITCH I...	FUNCTION	OPERA... ▲	VENDOR ...
›	10.0.11.1		10.0.11.1	9f85c219d7d0	1-Mgmt	10.0.11.1:Fa...			
›	ip-cam-axis-f33		10.0.14.73	0050c268c612	4-Facilities	10.0.14.1:Gi...	IP Camera		Axis Networ...
›	ip-cam-axis-f37		10.0.14.104	0050c2ac5082	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f38		10.0.14.127	0050c2816abf	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f32		10.0.14.155	0050c27f0a63	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f38		10.0.14.174	0050c2792f0b	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f38		10.0.14.255	0050c230b36f	4-Facilities	10.0.14.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f36		10.0.34.36	0050c2172b...	34-Facilities	10.0.34.1:Fa...	IP Camera		Axis Networ...
›	ip-cam-axis-f33		10.0.34.79	0050c2685288	34-Facilities	10.0.34.1:Gi...	IP Camera		Axis Networ...

Step 3: Scroll down the list and check Windows Desktop Zone.



Search...

Group: Windows Desktop Zone | ×

Filters — Clear All

- › Policies
- › Segments
- ⌄ Groups
  - Windows
  - ⌄ □ Corporate Hosts
    - › □ All Managed Windows De...
  - □ Exempt-Approved Windows ...
  - □ Unmanaged Windows Devices
  - □ Windows
  - ☑ Windows Desktop Zone
  - □ Windows Mobile

59 Results

	DEVICE ▲	DISPL...	IPV4 ADD...	MAC ADD...	SEGMENT	SWITCH I...	FUNCTION	OPERATI...	VENDOR ...
›	DEMOFS\W10	Alice Jones	10.0.2.10	0050560000...	Lab-Kit	10.0.1.9:Fa1/...	Computer	Windows 10	VMware
›	Desktop-32L8CB		10.0.33.130	f8db8884b4...	33-Guest	10.0.33.1:Gi...	Computer	Windows 7 ...	Dell
›	Desktop-38I2EJ	Michael L...	10.0.62.87	a69042ea85...	62-Production	10.0.62.1:Fa...	Computer	Windows 7 P...	Dell\Dell PC
›	Desktop-42I4ID		10.0.13.93	[illegible]	3-Guest	10.0.13.1:Fa...	Computer	Windows 7 ...	Dell
›	Desktop-65E6DA		[illegible]	f8db880107b7	3-Guest	10.0.13.1:Gi...	Computer	Windows 7 ...	Dell
›	Desktop-72B8GF	[illegible]	10.0.12.172	1a0c4dd36e...	2-Production	10.0.12.1:Gi...	Computer	Windows 7 P...	Dell\Dell PC
›	[illegible]		10.0.62.222	f8db8850b0...	62-Production	10.0.62.1:Fa...	Computer	Windows 7 ...	Dell
›	Desktop-84D9BH		10.0.63.225	f8db8840423f	63-Guest	10.0.63.1:Fa...	Computer	Windows 7 ...	Dell
›	Desktop-95C2JJ		10.0.62.103	f8db88d274...	62-Production	10.0.62.1:Gi...	Computer	Windows 7 ...	Dell

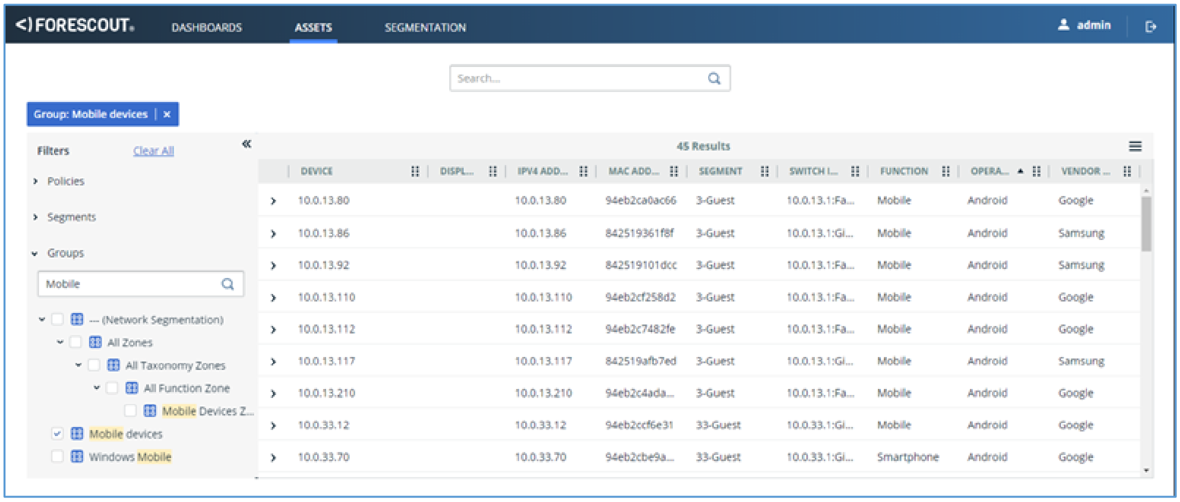
You can immediately see that you have some Windows 7 devices on your network.

Step 4: Click the **Operating System** column to sort by that column. Scroll down the list.

What other versions of Windows do you see?

Step 5: Click the caret to the left of one of the devices to see the device properties.

Step 6: Clear the filter and search for **Mobile** under Groups. Check the **Mobile devices** group.



Search...

Group: Mobile devices | ×

Filters — Clear All

- › Policies
- › Segments
- ⌄ Groups
  - Mobile
  - ⌄ □ — (Network Segmentation)
    - ⌄ □ All Zones
      - ⌄ □ All Taxonomy Zones
        - ⌄ □ All Function Zone
          - □ Mobile Devices Z...
  - ☑ Mobile devices
  - □ Windows Mobile

45 Results

	DEVICE	DISPL...	IPV4 ADD...	MAC ADD...	SEGMENT	SWITCH I...	FUNCTION	OPERA... ▲	VENDOR ...
›	10.0.13.80		10.0.13.80	94eb2ca0ac66	3-Guest	10.0.13.1:Fa...	Mobile	Android	Google
›	10.0.13.86		10.0.13.86	842519361f8f	3-Guest	10.0.13.1:Gi...	Mobile	Android	Samsung
›	10.0.13.92		10.0.13.92	842519101dcc	3-Guest	10.0.13.1:Fa...	Mobile	Android	Samsung
›	10.0.13.110		10.0.13.110	94eb2cf258d2	3-Guest	10.0.13.1:Fa...	Mobile	Android	Google
›	10.0.13.112		10.0.13.112	94eb2c7482fe	3-Guest	10.0.13.1:Fa...	Mobile	Android	Google
›	10.0.13.117		10.0.13.117	842519afb7ed	3-Guest	10.0.13.1:Gi...	Mobile	Android	Samsung
›	10.0.13.210		10.0.13.210	94eb2c4ada...	3-Guest	10.0.13.1:Fa...	Mobile	Android	Google
›	10.0.33.12		10.0.33.12	94eb2ccf6e31	33-Guest	10.0.33.1:Gi...	Mobile	Android	Google
›	10.0.33.70		10.0.33.70	94eb2cbe9a...	33-Guest	10.0.33.1:Gi...	Smartphone	Android	Google

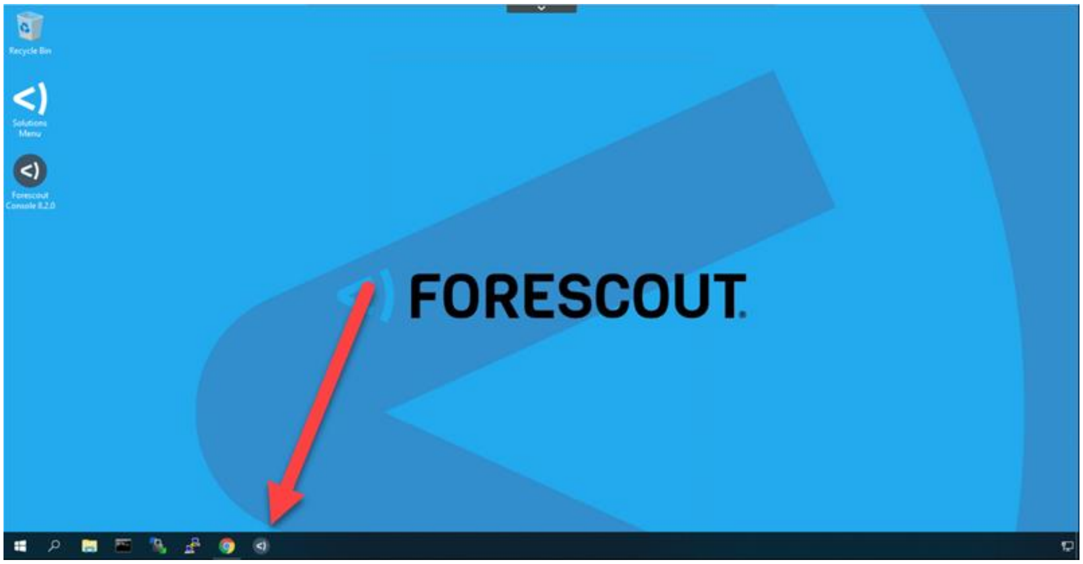
Step 7: Click the caret to the left of one of the devices to see the device properties.

Step 8: Use the filters to sort the Asset table in different ways. When you are done, clear any filters and click the **Dashboards** tab at the top of the page. Minimize the browser when you are done.

Task 2: Access the Forescout Console

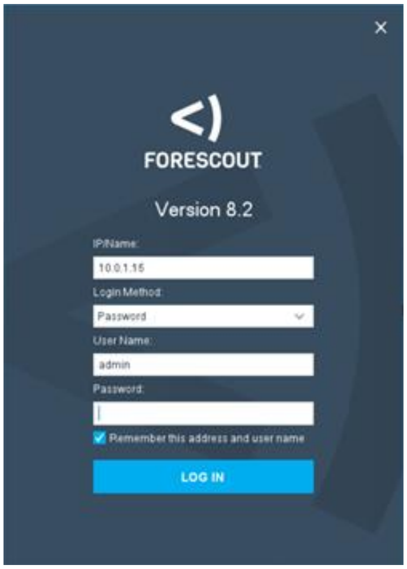
Up until now, we have done everything through the Forescout platform eyeSight dashboard. Now we are going to access the Forescout platform console.

Step 1: The Console Login dialog box should be running when you first access the console device. If it is not, click the **Forescout Console** icon <) in the taskbar.



The Console Login dialog appears.

Step 2: Enter **4Scout123** in the password field and press **Enter**. The password is case-sensitive.


FORESCOUT

Version 8.2

IP/Name: 10.0.1.15

Login Method: Password

User Name: admin

Password:

☑ Remember this address and user name

The Forescout Console opens.

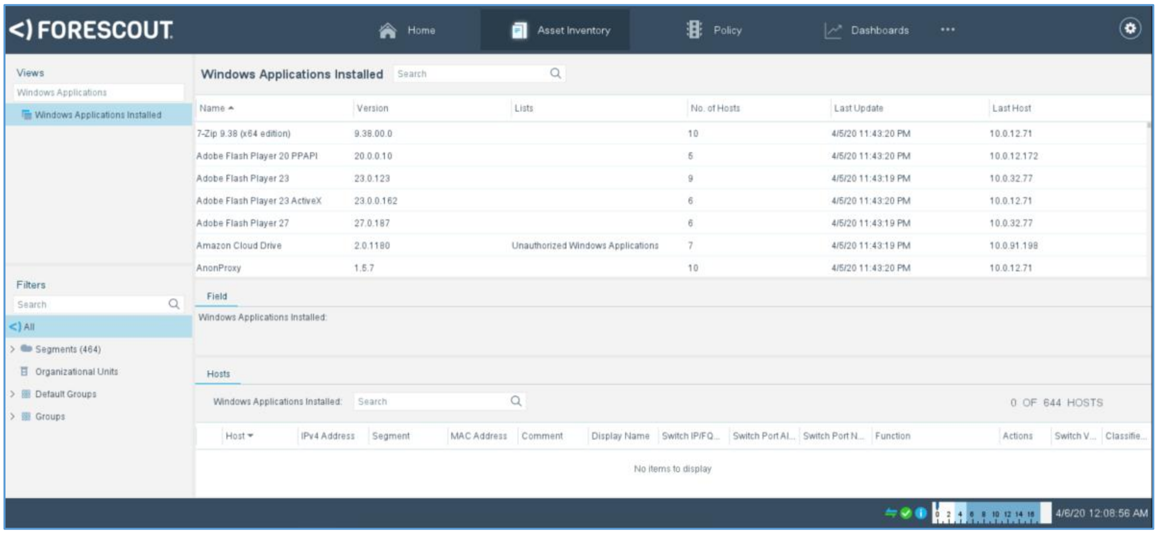
Task 3: See Microsoft Office Installations

Forescout can even tell you about software running on managed endpoints.

Step 1: Click the **Asset Inventory** tab at the top of the screen.

Step 2: In the **Views** tree, search for and select **Windows Applications Installed**.

A list of Windows applications and versions appears in the table on the right. The number of hosts on which each application is installed is also displayed.



Windows Applications Installed

Name ▲	Version	Lists	No. of Hosts	Last Update	Last Host
7-Zip 9.38 (x64 edition)	9.38.00.0		10	4/5/20 11:43:20 PM	10.0.12.71
Adobe Flash Player 20 PPAPI	20.0.0.10		5	4/5/20 11:43:20 PM	10.0.12.172
Adobe Flash Player 23	23.0.123		9	4/5/20 11:43:19 PM	10.0.32.77
Adobe Flash Player 23 ActiveX	23.0.0.162		6	4/5/20 11:43:20 PM	10.0.12.71
Adobe Flash Player 27	27.0.187		6	4/5/20 11:43:19 PM	10.0.32.77
Amazon Cloud Drive	2.0.1180	Unauthorized Windows Applications	7	4/5/20 11:43:19 PM	10.0.91.198
AnonProxy	1.5.7		10	4/5/20 11:43:20 PM	10.0.12.71

Windows Applications Installed:

Windows Applications Installed: 0 OF 644 HOSTS

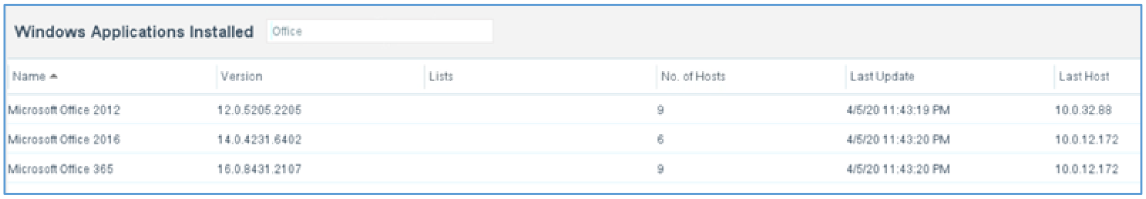
Host ▾	IPv4 Address	Segment	MAC Address	Comment	Display Name	Switch IP/FQ...	Switch Port Al...	Switch Port N...	Function	Actions	Switch V...	Classifie...

No items to display

4/6/20 12:08:56 AM

Step 3: In the Windows Applications Installed pane’s Search field, type **Office**.

The list is narrowed down to applications with Office in the name.



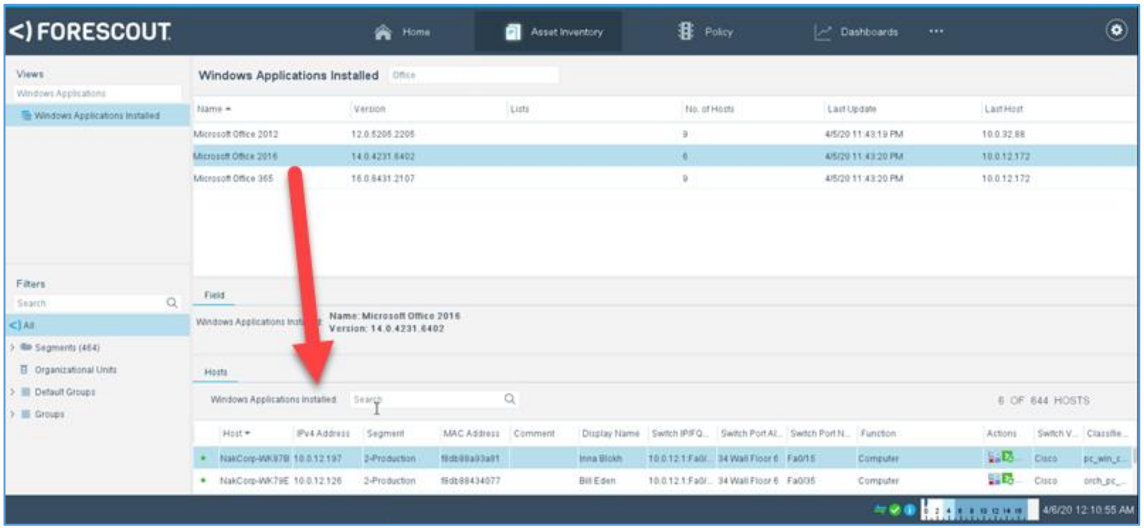
Windows Applications Installed Office

Name ▲	Version	Lists	No. of Hosts	Last Update	Last Host
Microsoft Office 2012	12.0.5205.2205		9	4/5/20 11:43:19 PM	10.0.32.88
Microsoft Office 2016	14.0.4231.6402		6	4/5/20 11:43:20 PM	10.0.12.172
Microsoft Office 365	16.0.8431.2107		9	4/5/20 11:43:20 PM	10.0.12.172

How many versions of Microsoft Office do you see? Does your company have a standard, licensed version?

Step 4: Click one of the versions of Microsoft Office.

A list of devices running that version of Office and their locations appear in the table below.



Windows Applications Installed: Office

Name	Version	Lists	No. of Hosts	Last Update	Last Host
Microsoft Office 2012	12.0.5205.2205		9	4/5/20 11:43:19 PM	10.0.32.88
Microsoft Office 2016	14.0.4231.6402		6	4/5/20 11:43:20 PM	10.0.12.172
Microsoft Office 365	16.0.8431.2107		9	4/5/20 11:43:20 PM	10.0.12.172

Windows Applications Installed: Name: Microsoft Office 2016
Version: 14.0.4231.6402

Windows Applications Installed — 6 OF 644 HOSTS

Host	IPv4 Address	Segment	MAC Address	Comment	Display Name	Switch IP/FQ...	Switch Port Al...	Switch Port N...	Function	Actions	Switch V...	Classifie...
NakCorp-WK87B	10.0.12.197	2-Production	f8db88a93a81		Inna Blokh	10.0.12.1:Fa0/...	34 Wall Floor 6	Fa0/15	Computer		Cisco	pc_win_c...
NakCorp-WK79E	10.0.12.126	2-Production	f8db88434077		Bill Eden	10.0.12.1:Fa0/...	34 Wall Floor 6	Fa0/35	Computer		Cisco	orch_pc_...

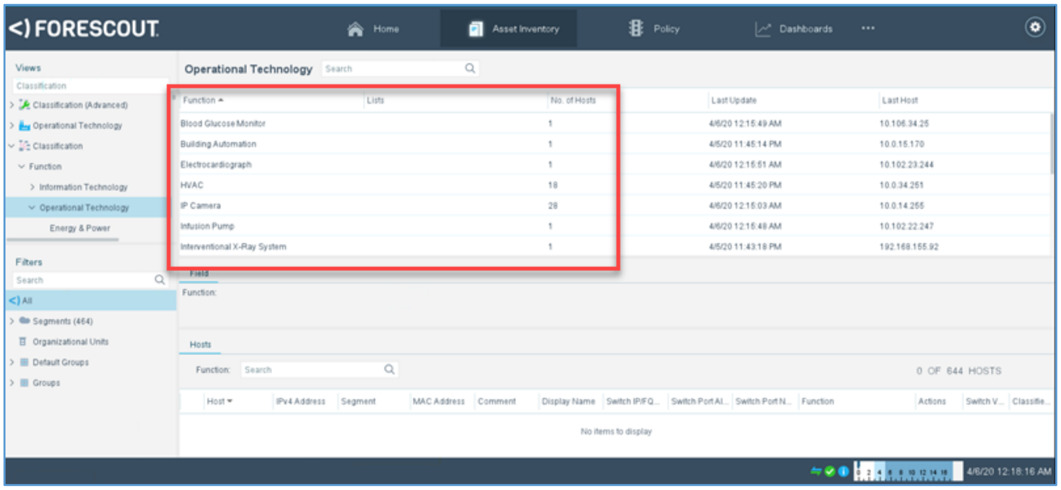
You can create policies for endpoints running specific versions of Microsoft Office. For example, you could notify users of an older version that they need to upgrade to the official, licensed version and where to obtain that version.

Task 4: See Your OT Devices

Step 1: In the Views tree, search for **Classification**. Expand it and click **Classification > Function > Operational Technology**.

NOTE: It is not the Classification (Advanced) entry. Collapse that entry to find the Classification entry.

A list of the categories of OT devices appears in Operational Technology table on the right.



Function ▲	Lists	No. of Hosts	Last Update	Last Host
Blood Glucose Monitor		1	4/6/20 12:15:49 AM	10.106.34.25
Building Automation		1	4/5/20 11:45:14 PM	10.0.15.170
Electrocardiograph		1	4/6/20 12:15:51 AM	10.102.23.244
HVAC		18	4/5/20 11:45:20 PM	10.0.34.251
IP Camera		28	4/6/20 12:15:03 AM	10.0.14.255
Infusion Pump		1	4/6/20 12:15:48 AM	10.102.22.247
Interventional X-Ray System		1	4/5/20 11:43:18 PM	192.168.155.92

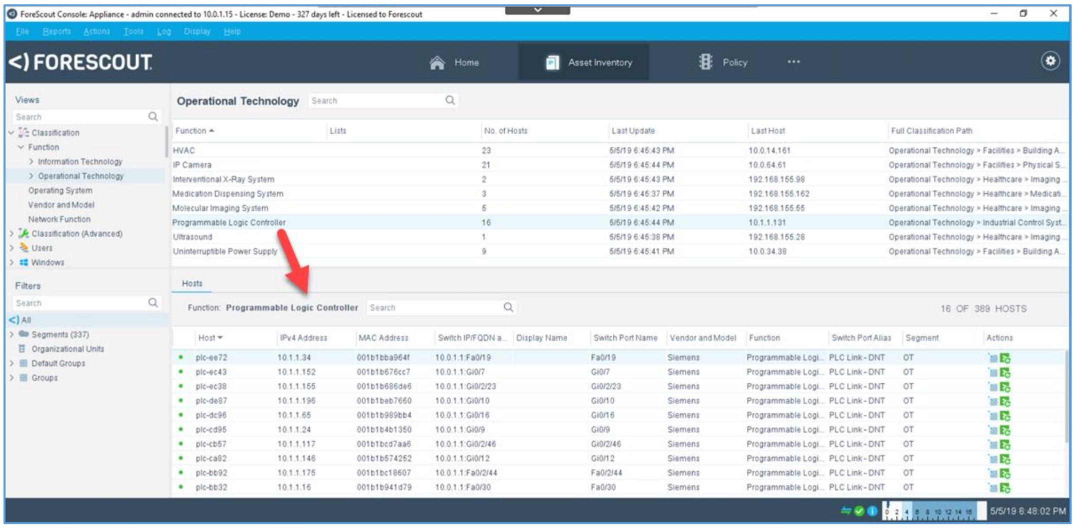
0 OF 644 HOSTS

Host ▼	IPv4 Address	Segment	MAC Address	Comment	Display Name	Switch IP/FQ...	Switch Port Al...	Switch Port N...	Function	Actions	Switch V...	Classifie...

No items to display

Step 2: Click **Programmable Logic Controller** in the Operational Technology table.

A list of the PLCs in your distribution center appears in the Hosts table.



Function ▲	Lists	No. of Hosts	Last Update	Last Host	Full Classification Path
HVAC		23	5/5/19 6:45:43 PM	10.0.14.161	Operational Technology > Facilities > Building A...
IP Camera		21	5/5/19 6:45:44 PM	10.0.64.61	Operational Technology > Facilities > Physical S...
Interventional X-Ray System		2	5/5/19 6:45:43 PM	192.168.155.98	Operational Technology > Healthcare > Imaging ...
Medication Dispensing System		3	5/5/19 6:45:37 PM	192.168.155.162	Operational Technology > Healthcare > Medicati...
Molecular Imaging System		5	5/5/19 6:45:42 PM	192.168.155.55	Operational Technology > Healthcare > Imaging ...
Programmable Logic Controller		16	5/5/19 6:45:44 PM	10.1.1.131	Operational Technology > Industrial Control Syst...
Ultrasound		1	5/5/19 6:45:38 PM	192.168.155.28	Operational Technology > Healthcare > Imaging ...
Uninterruptible Power Supply		9	5/5/19 6:45:41 PM	10.0.34.38	Operational Technology > Facilities > Building A...

Function: **Programmable Logic Controller**

16 OF 389 HOSTS

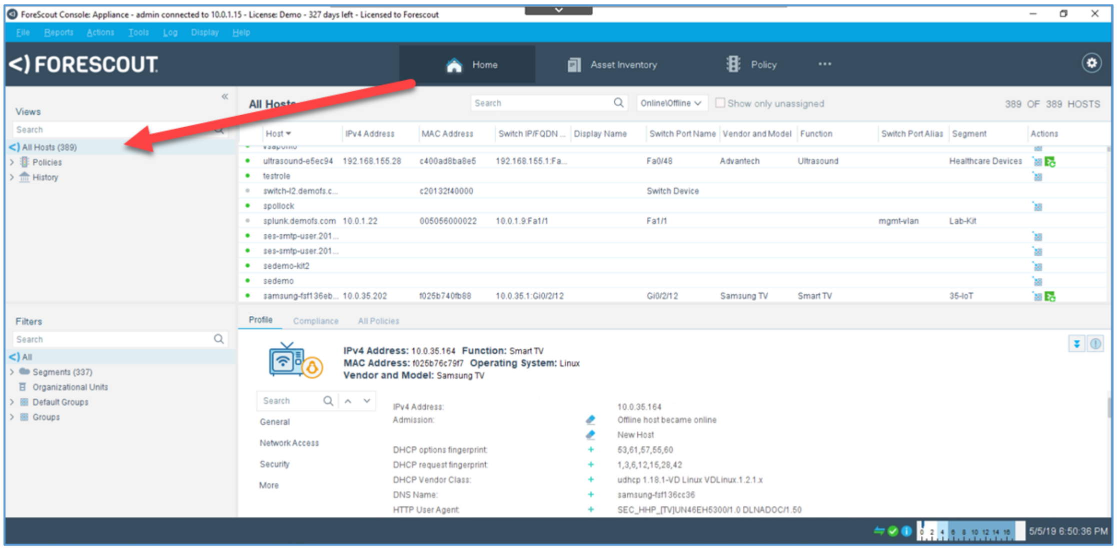
	Host ▼	IPv4 Address	MAC Address	Switch IP/FQDN a...	Display Name	Switch Port Name	Vendor and Model	Function	Switch Port Alias	Segment	Actions
●	plc-ee72	10.1.1.34	001b1bba964f	10.0.1.1:Fa0/19		Fa0/19	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-ec43	10.1.1.152	001b1b676cc7	10.0.1.1:Gi0/7		Gi0/7	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-ec38	10.1.1.155	001b1b686de6	10.0.1.1:Gi0/2/23		Gi0/2/23	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-de87	10.1.1.196	001b1beb7660	10.0.1.1:Gi0/10		Gi0/10	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-dc96	10.1.1.65	001b1b989bb4	10.0.1.1:Gi0/16		Gi0/16	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-cd95	10.1.1.24	001b1b4b1350	10.0.1.1:Gi0/9		Gi0/9	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-cb57	10.1.1.117	001b1bcd7aa6	10.0.1.1:Gi0/2/46		Gi0/2/46	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-ca82	10.1.1.146	001b1b574252	10.0.1.1:Gi0/12		Gi0/12	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-bb92	10.1.1.175	001b1bc18607	10.0.1.1:Fa0/2/44		Fa0/2/44	Siemens	Programmable Logi...	PLC Link - DNT	OT	
●	plc-bb32	10.1.1.16	001b1b941d79	10.0.1.1:Fa0/30		Fa0/30	Siemens	Programmable Logi...	PLC Link - DNT	OT	

Although this Hosts table shows specific types of OT devices, it does not show every device in your distribution center; it shows only the OT devices. The next task will show you how to see all the devices on your OT network segment.

Task 5: Monitor Your Distribution Center

Use the Home tab and segment filter to see the devices attached to your distribution center network. While the Inventory tab can help you see what devices you have on your network by type, the Home tab can help you see all the devices on specific parts of your network. This can help you track down unapproved devices on that network.

Step 1: Click the **Home** tab. If not already selected, click **All Hosts** in the Views tree.



All Hosts — Search — Online\Offline — ☐ Show only unassigned — 389 OF 389 HOSTS

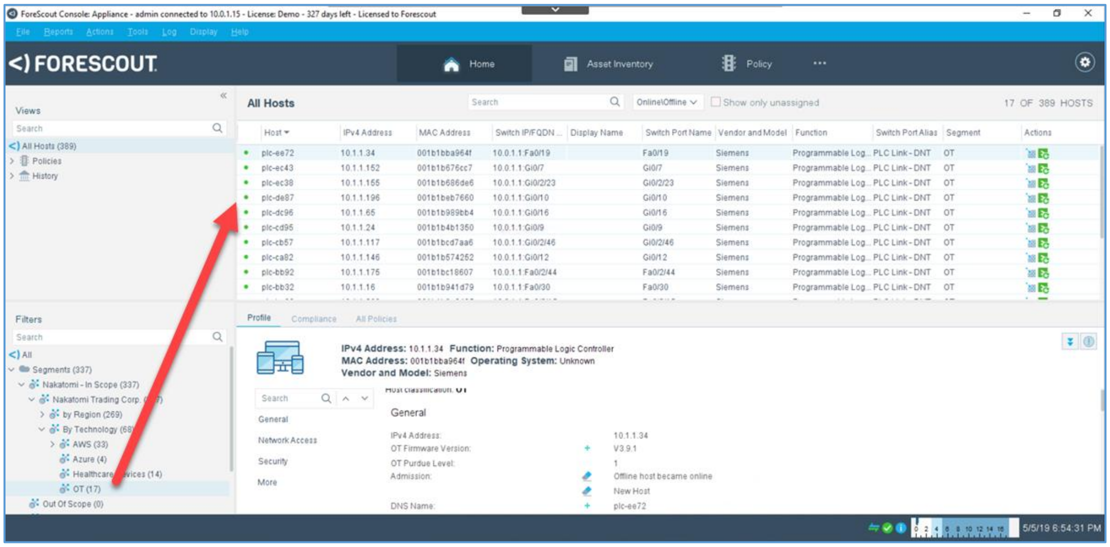
Host	IPv4 Address	MAC Address	Switch IP/FQDN ...	Display Name	Switch Port Name	Vendor and Model	Function	Switch Port Alias	Segment	Actions
ultrasound-e5ec94	192.168.155.28	c400ad8ba8e5	192.168.155.1:Fa...		Fa0/48	Advantech	Ultrasound		Healthcare Devices	
testrole										
switch-l2.demofs.c...		c20132f40000			Switch Device					
spollock										
splunk.demofs.com	10.0.1.22	005056000022	10.0.1.9:Fa1/1		Fa1/1			mgmt-vlan	Lab-Kit	
ses-smtp-user.201...										
ses-smtp-user.201...										
sedemo-kit2										
sedemo										
samsung-fsf136eb...	10.0.35.202	f025b740fb88	10.0.35.1:Gi0/2/12		Gi0/2/12	Samsung TV	Smart TV		35-IoT	

IPv4 Address: 10.0.35.164 **Function:** Smart TV
MAC Address: f025b76c79f7 **Operating System:** Linux
Vendor and Model: Samsung TV

IPv4 Address:	10.0.35.164
Admission:	Offline host became online
	New Host
DHCP options fingerprint:	53,61,57,55,60
DHCP request fingerprint:	1,3,6,12,15,28,42
DHCP Vendor Class:	udhcp 1.18.1-VD Linux VDLinux.1.2.1.x
DNS Name:	samsung-fsf136cc36
HTTP User Agent:	SEC_HHP_[TV]UN46EH5300/1.0 DLNADOC/1.50

Step 2: In the Filters tree, expand the **Segments > Nakatomi – In Scope > Nakatomi Trading Corp. > By Technology** tree, and then click **OT**.

In the All Hosts table, you will see a list of devices in your Distribution Center's OT network. You will be able to quickly identify devices that do not belong on this network.



All Hosts — Search — Online\Offline — ☐ Show only unassigned — 17 OF 389 HOSTS

Host	IPv4 Address	MAC Address	Switch IP/FQDN ...	Display Name	Switch Port Name	Vendor and Model	Function	Switch Port Alias	Segment	Actions
plc-ee72	10.1.1.34	001b1bba964f	10.0.1.1:Fa0/19		Fa0/19	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-ec43	10.1.1.152	001b1b676cc7	10.0.1.1:Gi0/7		Gi0/7	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-ec38	10.1.1.155	001b1b686de6	10.0.1.1:Gi0/2/23		Gi0/2/23	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-de87	10.1.1.196	001b1beb7660	10.0.1.1:Gi0/10		Gi0/10	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-dc96	10.1.1.65	001b1b989bb4	10.0.1.1:Gi0/16		Gi0/16	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-cd95	10.1.1.24	001b1b4b1350	10.0.1.1:Gi0/9		Gi0/9	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-cb57	10.1.1.117	001b1bcd7aa6	10.0.1.1:Gi0/2/46		Gi0/2/46	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-ca82	10.1.1.146	001b1b574252	10.0.1.1:Gi0/12		Gi0/12	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-bb92	10.1.1.175	001b1bc18607	10.0.1.1:Fa0/2/44		Fa0/2/44	Siemens	Programmable Log...	PLC Link - DNT	OT	
plc-bb32	10.1.1.16	001b1b941d79	10.0.1.1:Fa0/30		Fa0/30	Siemens	Programmable Log...	PLC Link - DNT	OT	

IPv4 Address: 10.1.1.34 **Function:** Programmable Logic Controller
MAC Address: 001b1bba964f **Operating System:** Unknown
Vendor and Model: Siemens

Host classification: OT

General

IPv4 Address:	10.1.1.34
OT Firmware Version:	V3.9.1
OT Purdue Level:	1
Admission:	Offline host became online
	New Host
DNS Name:	plc-ee72

Step 3: Scroll through the device list. Are there any devices that you can immediately see that do not belong?

Hint: Look at the function column as you scroll through. Looks like someone is doing some after-hours gaming. There is an Xbox on your OT network.

Step 4: Click the **Asset Inventory** tab to return to the Inventory view.

Follow Up

- What types of information did Forescout discover about the devices?
- How could seeing all instances of a specific device type on your network, such as IT, OT, and IoT devices, benefit your business? Open ports?
- What problems does your organization currently face that this type of endpoint visibility could help solve? How much effort and expense currently goes into solving these problems?
- How can Forescout help you keep your asset inventory current?

Lap 3: Incident Response

Scenario

Part way through your Forescout proof of value, a malware outbreak, WannaCry ransomware, goes global.

You need to see if any of your endpoints are infected with or vulnerable to WannaCry and pinpoint exactly where they are. Unfortunately, it is a zero-day outbreak, and your malware software does not yet detect WannaCry.

Luckily, the SE you are working with at Forescout is already aware of this outbreak. The SE sent you policies you can use to discover infected and vulnerable endpoints and locate where they are within your company.

Leveraging these policies, you discover that you have several endpoints that are vulnerable, but also some that are already infected.

Because the Forescout platform can identify the switches and switch ports that endpoints are plugged into, you can quickly identify the location of any endpoint.

Couple this capability with a control or orchestration policy, and you can quickly hunt for and isolate compromised or vulnerable locations or have your vulnerability scanners scan the potentially affected endpoints.

Forescout can then use a virtual firewall, VLAN reassignment or orchestration with your other security products to isolate the infected systems.

Before you begin

- How do you hunt for vulnerable systems and possibly compromised locations for zero-day threats?
- What is your process for addressing those systems and locations?
- What is the impact of undiscovered infected or vulnerable endpoints to your organization? How long does it take you to find them now?
- How does the problem/risk to the organization become worse as time elapses?

In this lap, you will:

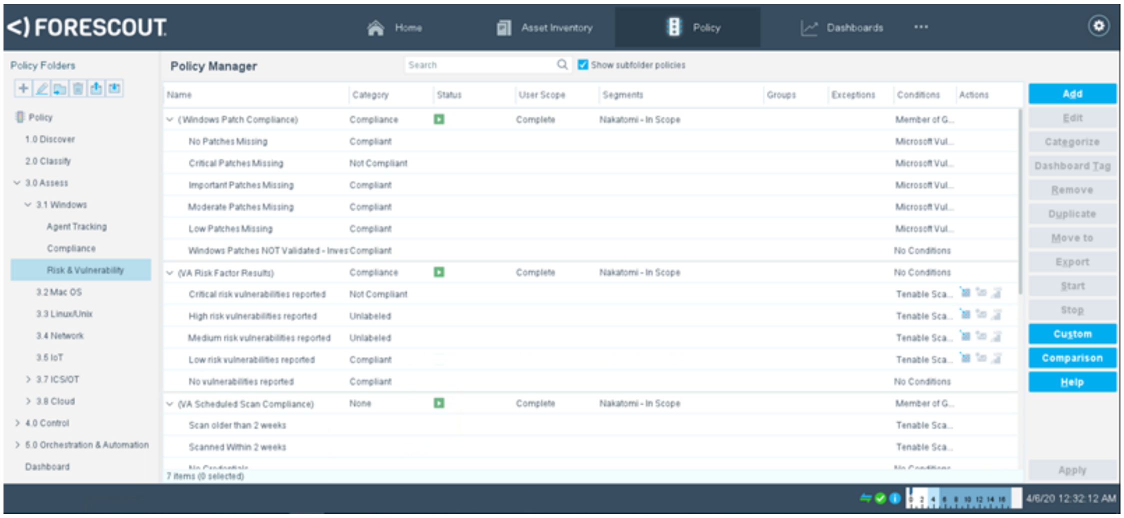
1. Import a policy to identify endpoints possibly infected by the malware outbreak.
2. Import a policy to identify endpoints vulnerable to it.
3. Create a dashboard to monitor the progress in addressing this outbreak.

Task 1: Import the WannaCry Policy

This policy looks for specific characteristics on endpoints that indicate a WannaCry infection.

Step 1: Click the **Policy** tab in the Forescout console toolbar.

Step 2: In the **Policy Folders** tree, expand **3.0 Assess > 3.1 Windows** and click **Risk & Vulnerability**.



Policy Manager

Search ☑ Show subfolder policies

Name	Category	Status	User Scope	Segments	Groups	Exceptions	Conditions	Actions
(Windows Patch Compliance)	Compliance	▶	Complete	Nakatomi - In Scope			Member of G...	
No Patches Missing	Compliant						Microsoft Vul...	
Critical Patches Missing	Not Compliant						Microsoft Vul...	
Important Patches Missing	Compliant						Microsoft Vul...	
Moderate Patches Missing	Compliant						Microsoft Vul...	
Low Patches Missing	Compliant						Microsoft Vul...	
Windows Patches NOT Validated - Inves	Compliant						No Conditions	
(VA Risk Factor Results)	Compliance	▶	Complete	Nakatomi - In Scope			No Conditions	
Critical risk vulnerabilities reported	Not Compliant						Tenable Sca...	
High risk vulnerabilities reported	Unlabeled						Tenable Sca...	
Medium risk vulnerabilities reported	Unlabeled						Tenable Sca...	
Low risk vulnerabilities reported	Compliant						Tenable Sca...	
No vulnerabilities reported	Compliant						No Conditions	
(VA Scheduled Scan Compliance)	None	▶	Complete	Nakatomi - In Scope			Member of G...	
Scan older than 2 weeks							Tenable Sca...	
Scanned Within 2 weeks							Tenable Sca...	
No Credentials							No Conditions	

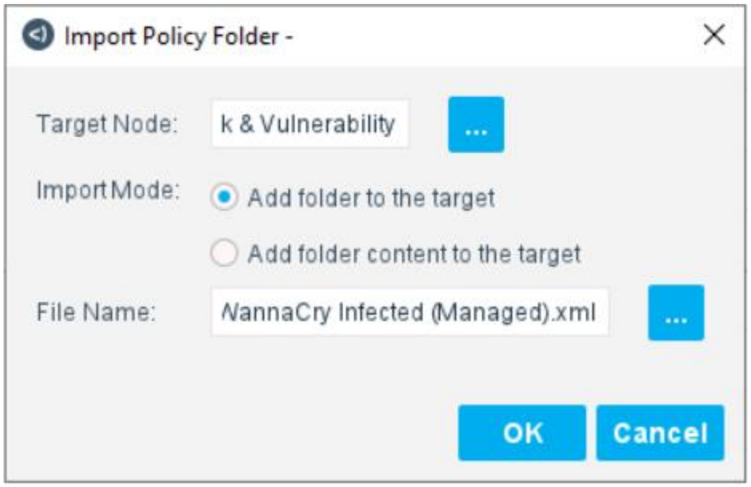
7 items (0 selected)

Step 3: Click the **Import Policy Folder** icon .

The Select Policy Folder dialog appears.

Step 4: Keep the Target Node at Risk & Vulnerability. Select **Add folder content to the target** under the Import Mode.

Step 5: Click the file browse button next to file name and navigate to the **Documents > Forescout Policies** folder. Select the **WannCry Infected (Managed).xml** file.



Import Policy Folder -

Target Node: k & Vulnerability

Import Mode: ● Add folder to the target

○ Add folder content to the target

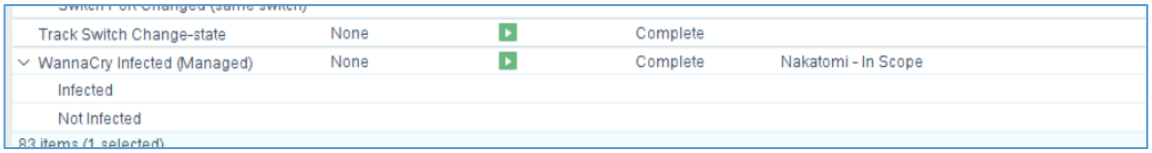
File Name: NannaCry Infected (Managed).xml

Step 6: Click **OK**.

The Policy detail dialog box appears.

Step 7: Click **OK**.

The policy is added to the bottom of the eyeSight policies. You can scroll down to see the policy at the bottom of the list.



Switch Port Changed (Same Switch)				
Track Switch Change-state	None	▶	Complete	
WannaCry Infected (Managed)	None	▶	Complete	Nakatomi - In Scope
Infected				
Not Infected				

83 items (1 selected)

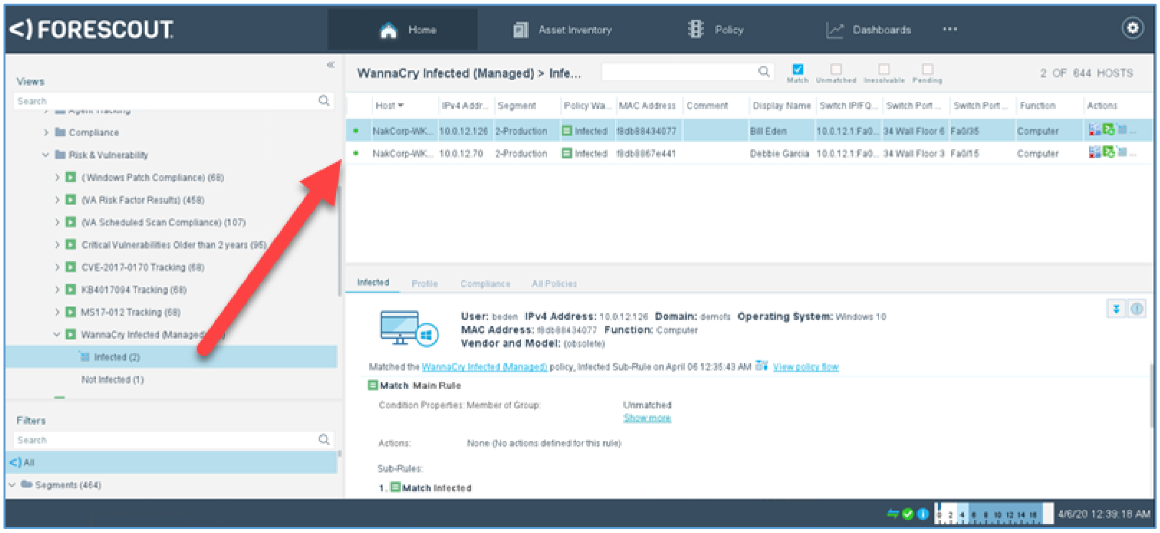
Step 8: Click **Apply**.

Step 9: Click the **Home** tab at the top of the screen.

Step 10: Expand the Policy tree: **Policies > 3.0 Assess > 3.1 Windows > Risk & Vulnerability > WannaCry Infected (Managed)**.

Step 11: Click **Infected**.

Now you will see a list of hosts with properties that indicate a WannaCry infection. Furthermore, you can see which switch and port they are attached to.



	Host	IPv4 Addr...	Segment	Policy Wa...	MAC Address	Comment	Display Name	Switch IP/FQ...	Switch Port ...	Switch Port ...	Function	Actions
●	NakCorp-WK...	10.0.12.126	2-Production	Infected	f8db88434077		Bill Eden	10.0.12.1:Fa0...	34 Wall Floor 6	Fa0/35	Computer	...
●	NakCorp-WK...	10.0.12.70	2-Production	Infected	f8db8867e441		Debbie Garcia	10.0.12.1:Fa0...	34 Wall Floor 3	Fa0/15	Computer	...

User: beden **IPv4 Address:** 10.0.12.126 **Domain:** demofs **Operating System:** Windows 10
MAC Address: f8db88434077 **Function:** Computer
Vendor and Model: (obsolete)

Matched the WannaCry Infected (Managed) policy, Infected Sub-Rule on April 06 12:35:43 AM View policy flow

Match Main Rule

Condition Properties: Member of Group: Unmatched
Show more

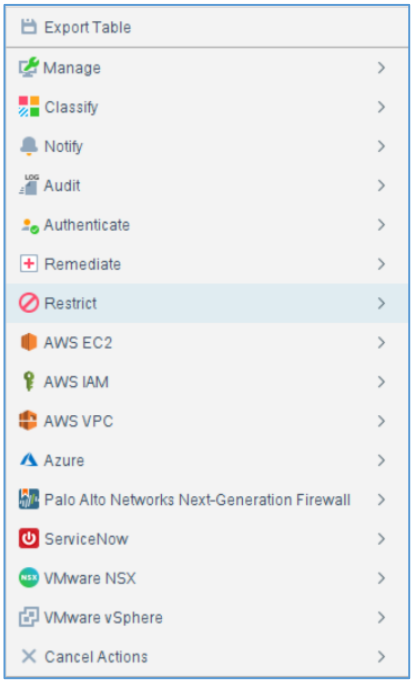
Actions: None (No actions defined for this rule)

Sub-Rules:

1. **Match Infected**

Now that you have identified the infected hosts, there are several things you can do:

- Take immediate action on each device by right-clicking the device and selecting an action, such as restricting network access either by assigning the endpoint to a quarantine VLAN or by using a virtual firewall to block it.



- Modify the policy to automatically block those devices from accessing the network.
- Locate the devices and send a support team to remediate them.

We are not going to take any action on these devices in this lap.

Task 2: Install the EternalBlue Vulnerability Policy

It is not enough to identify the infected devices. You also want to know which devices are vulnerable to WannaCry. WannaCry takes advantage of the EternalBlue exploit, which is a vulnerability in the Microsoft implementation of the SMB protocol. This vulnerability has been patched. This policy detects endpoints that are still vulnerable to the exploit.

Step 1: Click the **Policy** tab in the Forescout console toolbar.

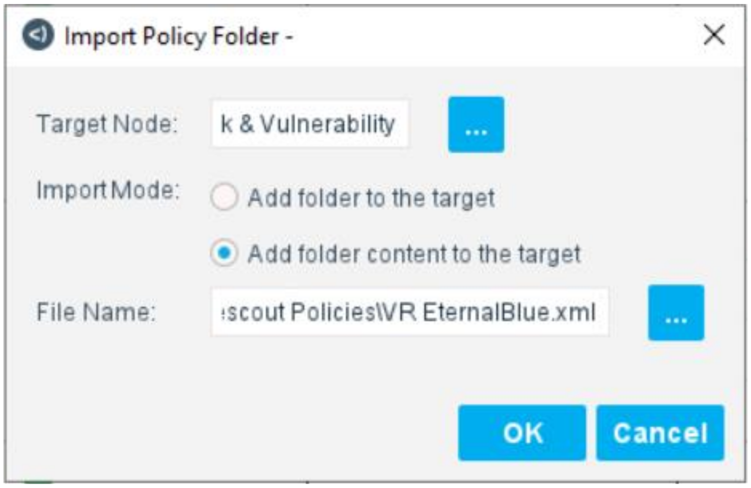
You should still be in the Risk & Assessment folder.

Step 2: Click the **Import Policy Folder** icon .

The Select Policy Folder dialog appears.

Step 3: Keep the Target Node at 1.0 See. Select **Add folder content to the target** under the Import Mode.

Step 4: Click the file browser button next to file name and navigate to the **Documents > Policies** folder. Select the **VR EternalBlue vulnerable.xml** file.



Import Policy Folder -

Target Node: k & Vulnerability

Import Mode: ○ Add folder to the target
● Add folder content to the target

File Name: ᵎscout Policies\VR EternalBlue.xml

Step 5: Click **OK**.

The Policy detail dialog box appears.

Step 6: Click **OK**.

The policy is added to the bottom of the list of policies.

Step 7: Click **Apply**.

Step 8: Click the **Home** tab at the top of the screen.

Step 9: Expand the **VR EternalBlue** policy (it should appear above the WannaCry policy in the tree)

Step 10: Click **Vulnerable**.

You will see a list of devices that are still vulnerable to this exploit, and therefore to WannaCry.

Like the WannaCry-infected devices, you can take several steps to remediate these devices. You could use policy to:

- Quarantine them to a remediation VLAN.
- Start the update process so that they receive the required patches.
- Notify the users of the vulnerabilities.

We are not going to take any action on these devices in this task.

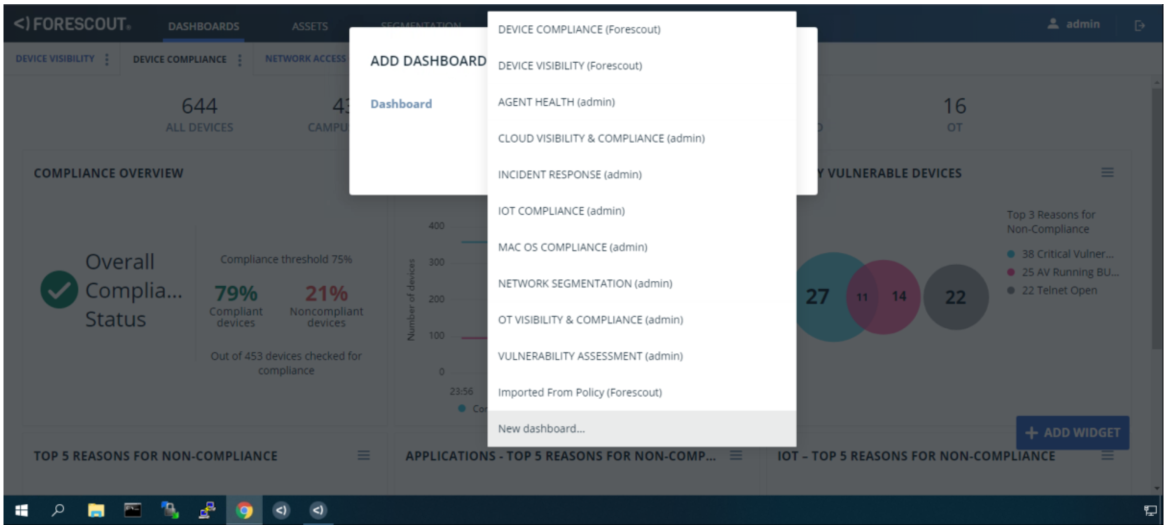
Task 3: Add WannaCry-Infected and Vulnerable Hosts to the Dashboard

Because of the critical importance of this issue to your company, you are going to create a custom dashboard to track the progress in identifying and eliminating infected and vulnerable systems.

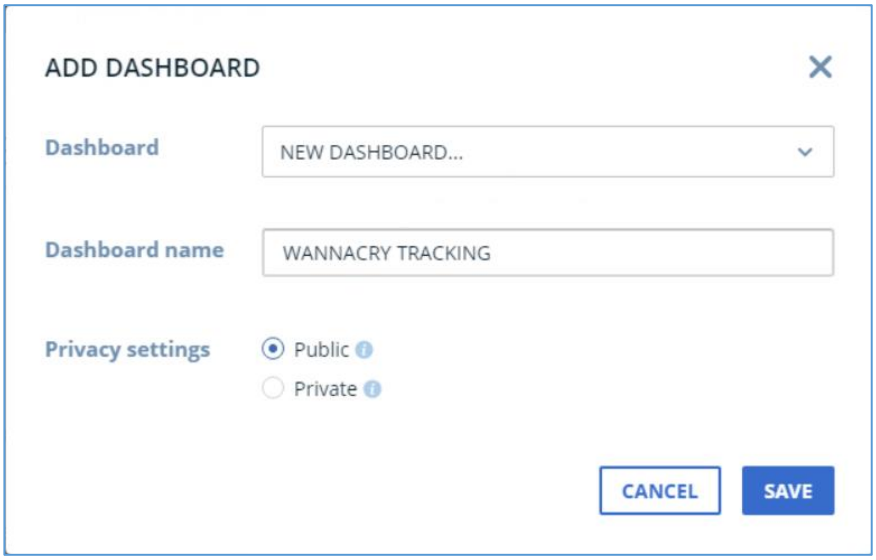
Step 1: Open the browser. If the Dashboards tab is not showing, click **Dashboards** at the top of the page.

Step 2: Click the **Add Dashboard** (**+**) icon to the right of the dashboard names at the top of the page.

The Add Dashboard dialog appears.


FORESCOUT
DASHBOARDS
ASSETS
admin
DEVICE VISIBILITY
DEVICE COMPLIANCE
NETWORK ACCESS
ADD DASHBOARD
Dashboard
DEVICE COMPLIANCE (Forescout)
DEVICE VISIBILITY (Forescout)
AGENT HEALTH (admin)
CLOUD VISIBILITY & COMPLIANCE (admin)
INCIDENT RESPONSE (admin)
IOT COMPLIANCE (admin)
MAC OS COMPLIANCE (admin)
NETWORK SEGMENTATION (admin)
OT VISIBILITY & COMPLIANCE (admin)
VULNERABILITY ASSESSMENT (admin)
Imported From Policy (Forescout)
New dashboard...
644
ALL DEVICES
16
OT
COMPLIANCE OVERVIEW
Overall Complia... Status
Compliance threshold 75%
79% Compliant devices
21% Noncompliant devices
Out of 453 devices checked for compliance
VULNERABLE DEVICES
Top 3 Reasons for Non-Compliance
38 Critical Vulner...
25 AV Running BU...
22 Telnet Open
27
11
14
22
+ ADD WIDGET
TOP 5 REASONS FOR NON-COMPLIANCE
APPLICATIONS - TOP 5 REASONS FOR NON-COMP...
IOT - TOP 5 REASONS FOR NON-COMPLIANCE

Step 3: Name your dashboard and select **Public** for the privacy setting. This will enable other users to see the dashboard.



ADD DASHBOARD ✕

Dashboard: NEW DASHBOARD...

Dashboard name: WANNACRY TRACKING

Privacy settings: ● Public ○ Private

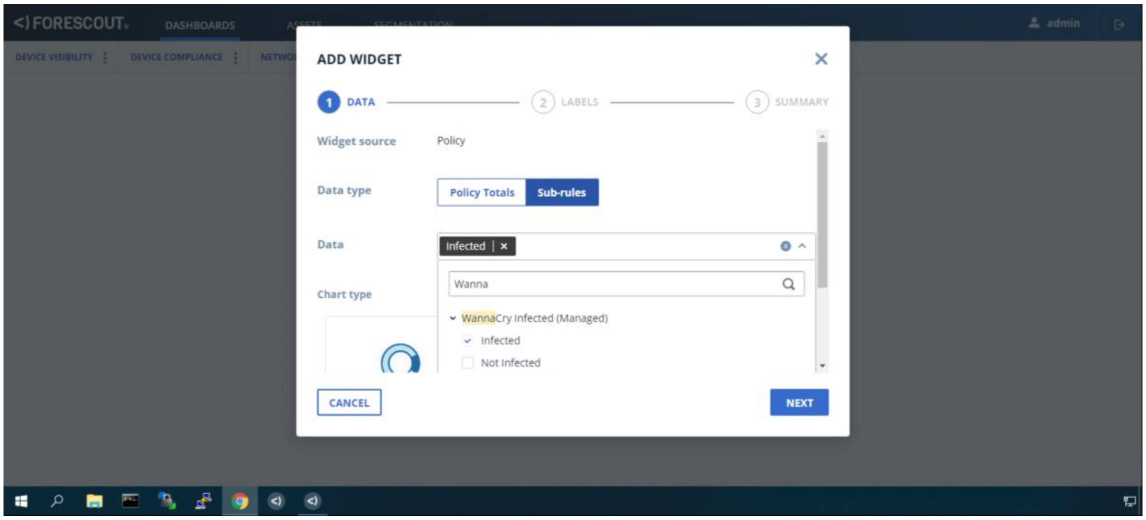
CANCEL SAVE

Step 4: Click **Save**.

Your new dashboard is created, but it is empty. Let’s add some widgets.

Step 5: Click the **+ Add Widget** button.

The Add Widget wizard appears.



ADD WIDGET

Widget source: Policy

Data type: Policy Totals | Sub-rules

Data: Infected

Wanna

- WannaCry Infected (Managed)
  - ✓ Infected
  - □ Not Infected

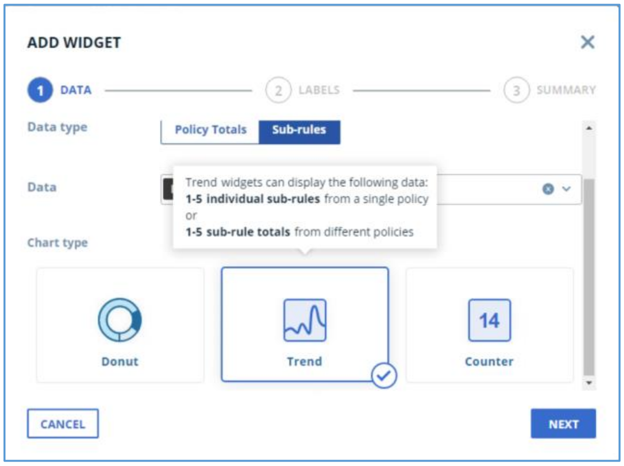
Step 6: Select **Sub Rules** for the Data Type.

Step 7: Click in the Data field and search for WannaCry. Select the **Infected** checkbox.

Infected is added to the Data field.

Step 8: Click the caret at the right of the Data field to close the search fields.

Step 9: Select Trend as the Chart type.



ADD WIDGET

Data type: Policy Totals | Sub-rules

Trend widgets can display the following data:
1-5 individual sub-rules from a single policy
or
1-5 sub-rule totals from different policies

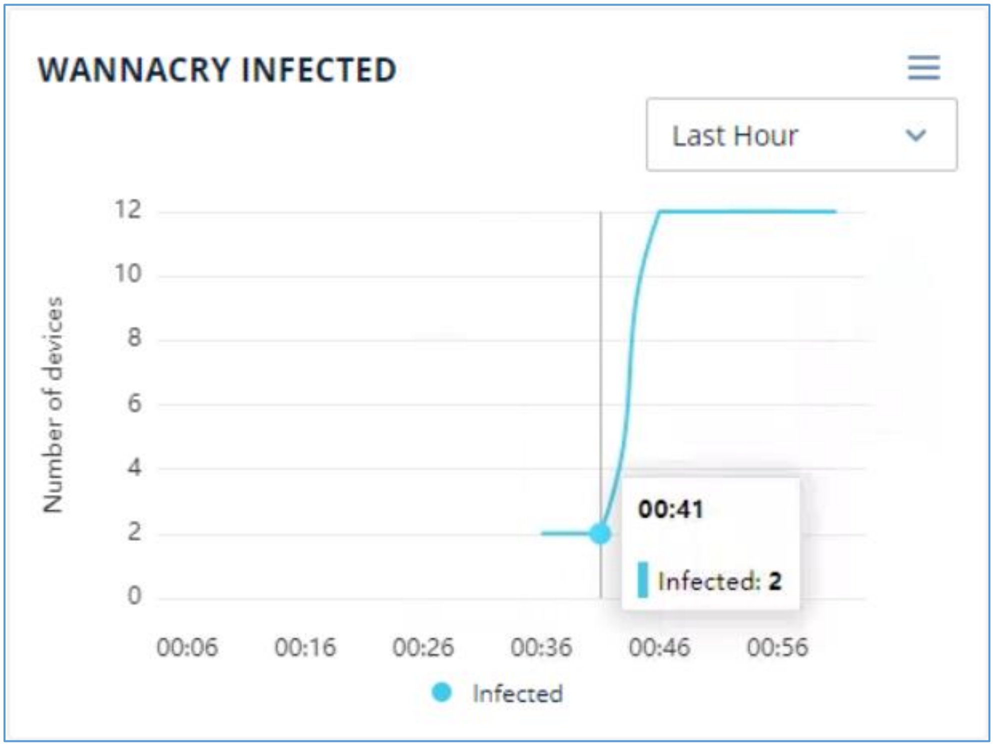
Chart type: Trend

Step 10: Click **Next**.

Step 11: Give your policy a name and click **Next**.

Step 12: Review the policy summary and click **Finish**.

Your widget is added to the Dashboard. It may take a minute to populate. It shows the number of WannaCry-infected devices over time, enabling you to track your progress in eliminating the threat. You can change the chart's timeframe using the drop-down menu.



Over time, as additional hosts become infected, or as infected hosts are remediated, this widget will enable you to track your progress in addressing this incident.

Step 13: Now try adding a widget using the above steps for the **VR EternalBlue** policy. Use the **Vulnerable** sub-rule.

Step 14: Minimize the web browser when you are done.

Follow Up

- How can the Forescout platform affect your response time for zero-day threats and vulnerabilities? How would a faster response time benefit your business?
- How would the ability to automatically act on compromised or vulnerable endpoints change the way you currently address vulnerabilities?

Lap 4: Segmentation

Scenario

Although the Forescout platform helped you quickly gain control during the WannaCry outbreak on your network, you realize that you need to reduce the attack surface on your network to slow the spread or even stop these types of threats. You need to ensure that your devices only have access to the resources they need and nothing more.

You know that Forescout has a product, eyeSegment, that helps you design, plan, and deploy dynamic segmentation across the extended enterprise. You contact your Forescout Sales Engineer to start a trial of that product. Your SE helps you to define some basic eyeSegment policies for your network.

Network segmentation is not a one-time project. As your network grows and evolves, you need to constantly monitor, adapt, and grow revise your segmentation strategy.

eyeSegment simplifies the process of creating context-aware segmentation policies. It facilitates visualization and simulation of policies—prior to enforcement—for proactive finetuning and validation. You can see the traffic flowing between the various parts of your network, design segmentation polices for that traffic, and simulate the impact of those policies before implementing them. Then you can implement control across diverse enforcement technologies and network domains through a single policy framework.

Before you begin

- How do you currently monitor the communication between the various parts of your extended enterprise network?
- What is your current segmentation strategy? How do you enforce it uniformly across your different network technologies?
- What challenges are you currently facing in your segmentation efforts? How are you minimizing the possibility of business disruption during the rollout of your segmentation project?

In this lap, you will:

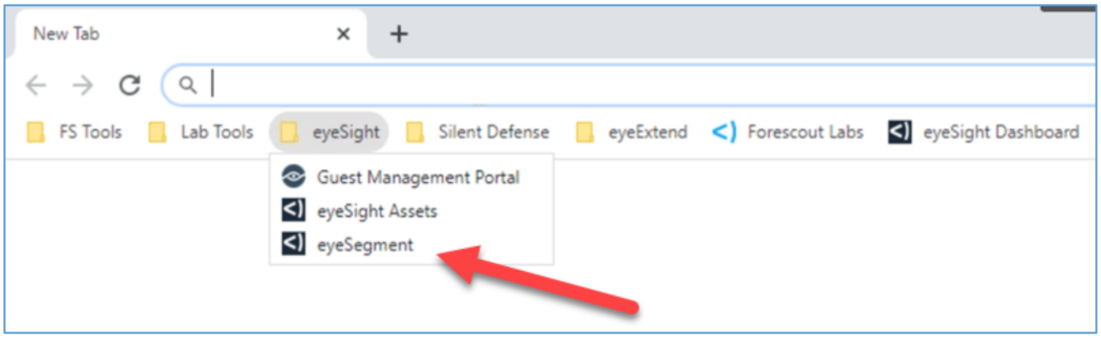
1. Use eyeSegment to visualize the traffic on the network.
2. Identify a traffic flow that should not be occurring.
3. Modify an eyeSegment policy to enable some traffic.
4. Create a policy to address the traffic that violates the segmentation rules.

Task 1: Visualize Your Network Traffic

In this task you will examine the traffic flows on your network.

Step 1: Open the Chrome browser from the console devices taskbar.

Step 2: If you still have the Dashboard open, click the **Segmentation** tab. Otherwise, from the bookmark bar, select **eyeSight > eyeSegment**.

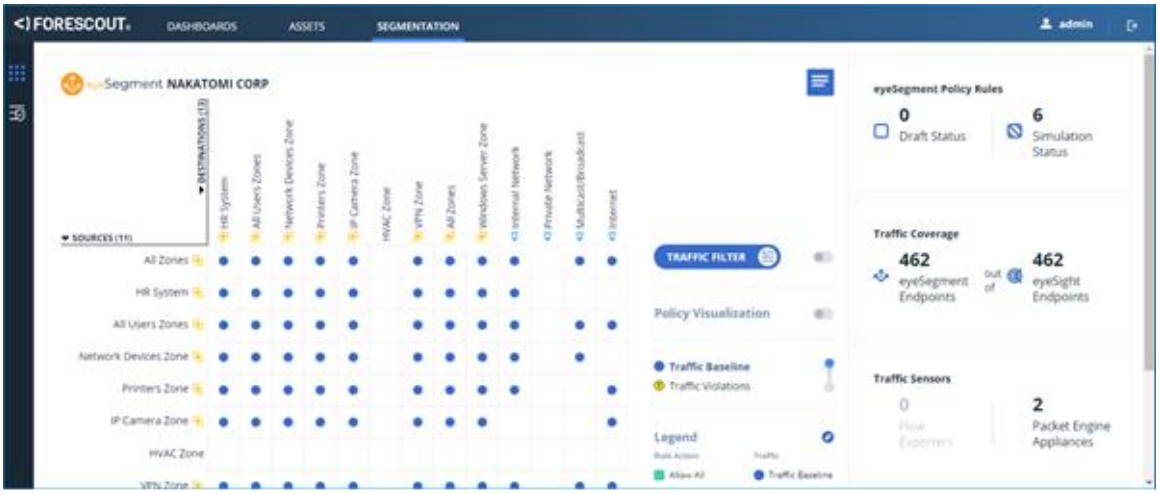


The eyeSegment login page appears.

Step 3: Log in with the prepopulated credentials. If the credentials are not already populated in the login fields, use the following:

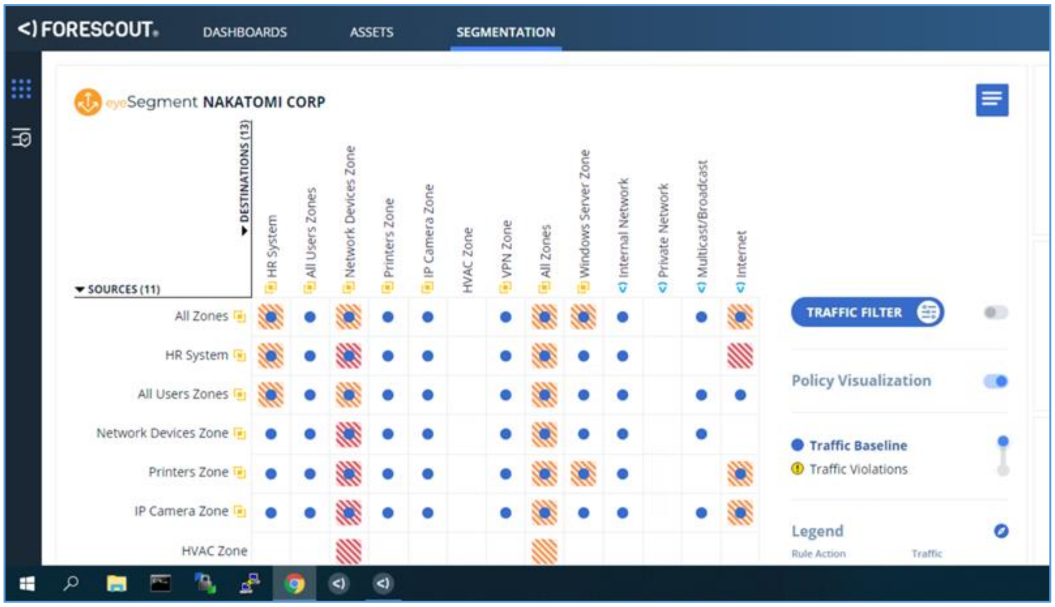
Username: admin
Password: 4Scout123

The eyeSegment matrix appears. The matrix shows traffic sources down the left and destinations across the top. A dot in a cell indicate that traffic was detected from the source to the destination indicated by the cell. You can easily see where your traffic is coming from and where it is going to. You can also see how many endpoints seen with eyeSight all covered by the traffic matrix.



SOURCES (11) \ DESTINATIONS (13)	HR System	All Users Zones	Network Devices Zone	Printers Zone	IP Camera Zone	HVAC Zone	VPN Zone	All Zones	Windows Server Zone	Internal Network	Private Network	Multicast/Broadcast	Internet
All Zones	●	●	●	●	●		●	●	●	●		●	●
HR System	●	●	●	●	●		●	●	●	●			
All Users Zones	●	●	●	●	●		●	●	●	●		●	●
Network Devices Zone	●	●	●	●	●		●	●	●	●		●	
Printers Zone	●	●	●	●	●		●	●	●	●			●
IP Camera Zone	●	●	●	●	●		●	●	●				●
HVAC Zone													
VPN Zone	●	●	●	●	●		●	●	●	●		●	●

Step 4: Click the **Policy Visualization** toggle to see which traffic is being affected by your segmentation rules.



SOURCES (11) \ DESTINATIONS (13)	HR System	All Users Zones	Network Devices Zone	Printers Zone	IP Camera Zone	HVAC Zone	VPN Zone	All Zones	Windows Server Zone	Internal Network	Private Network	Multicast/Broadcast	Internet
All Zones	🟧●	●	🟧●	●	●		●	🟧●	🟧●	●		●	🟧●
HR System	🟧●	●	🟥●	●	●		●	🟧●	●	●			🟥
All Users Zones	🟧●	●	🟧●	●	●		●	🟧●	●	●		●	●
Network Devices Zone	●	●	🟥●	●	●		●	🟧●	●	●		●	
Printers Zone	●	●	🟥●	●	●		●	🟧●	🟧●	●			🟧●
IP Camera Zone	●	●	🟥●	●	●		●	🟧●	●	●		●	🟧●
HVAC Zone			🟥					🟧					

The red indicates that all the traffic seen would be denied by your segmentation policy. The orange indicates that some of the traffic seen between those would be affected by your segmentation policy.

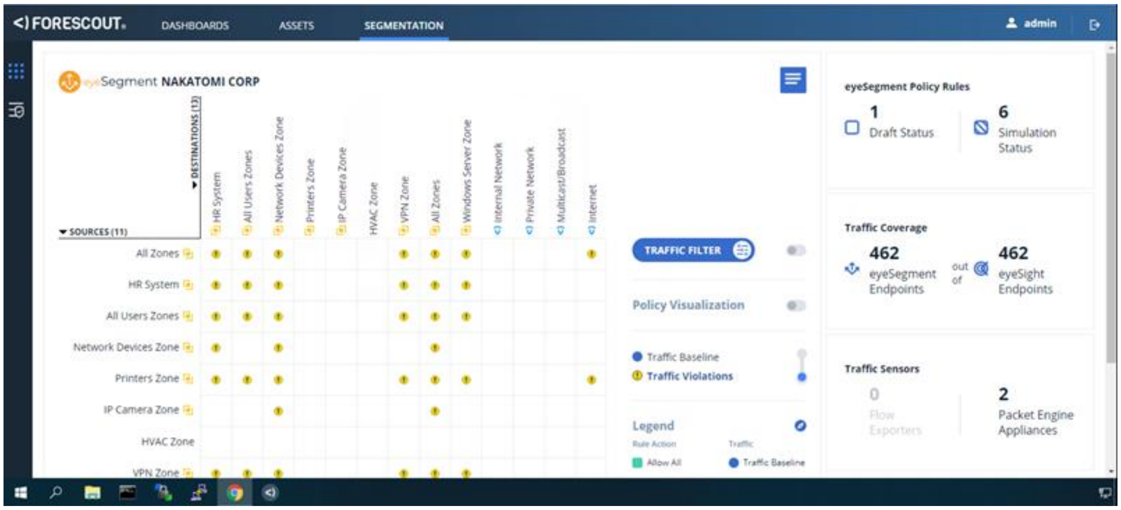
Step 5: Click the **Policy Visualization** toggle again to turn off the overlay.

Task 2: Identify Segmentation Rule Violations

There is a lot of traffic shown in the matrix. However, eyeSegment makes it easy to find the traffic that violates the rules that you configured.

Step 1: To the right of the eyeSegment matric, click the circle next to **Traffic Violations**.

The matrix displays an exclamation point in the cells that contain traffic that violates your segmentation rules.



eyeSegment Policy Rules
1 Draft Status
6 Simulation Status

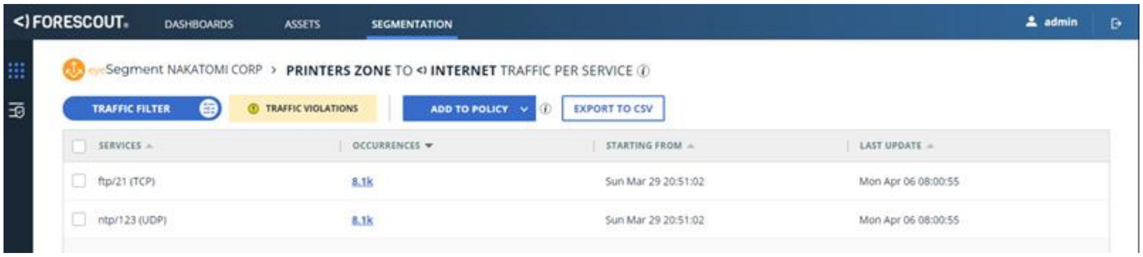
Traffic Coverage
462 eyeSegment Endpoints out of 462 eyeSight Endpoints

Traffic Sensors
0 Flow Exporters
2 Packet Engine Appliances

One thing that immediately stands out to you is that your printers are sending information to the Internet zone.

Step 2: Double-click the cell at the intersection of the Printer Zone and the Internet.

A table of the traffic from the Printer Zone to the Internet appears.



SERVICES	OCCURRENCES	STARTING FROM	LAST UPDATE
ftp/21 (TCP)	8.1k	Sun Mar 29 20:51:02	Mon Apr 06 08:00:55
ntp/123 (UDP)	8.1k	Sun Mar 29 20:51:02	Mon Apr 06 08:00:55

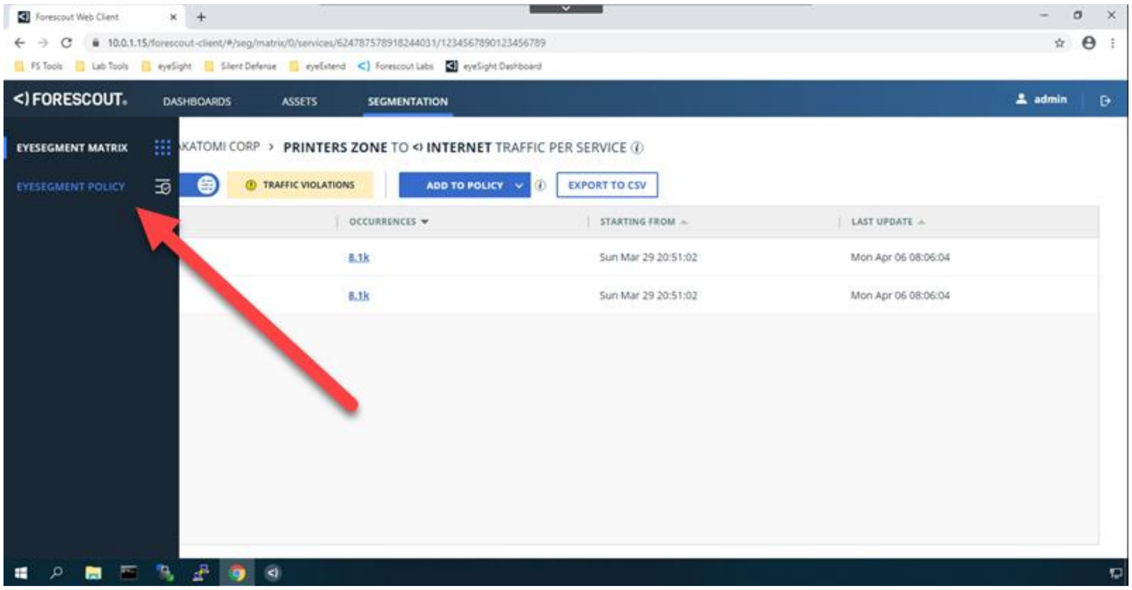
Step 3: If you want to see more detail about the traffic, click the **Occurrences** value.

You can see the traffic broken down by source IP, the timeframe when the traffic was seen, and more. What other types of information can you see?

Task 3: Modify an eyeSegment Policy

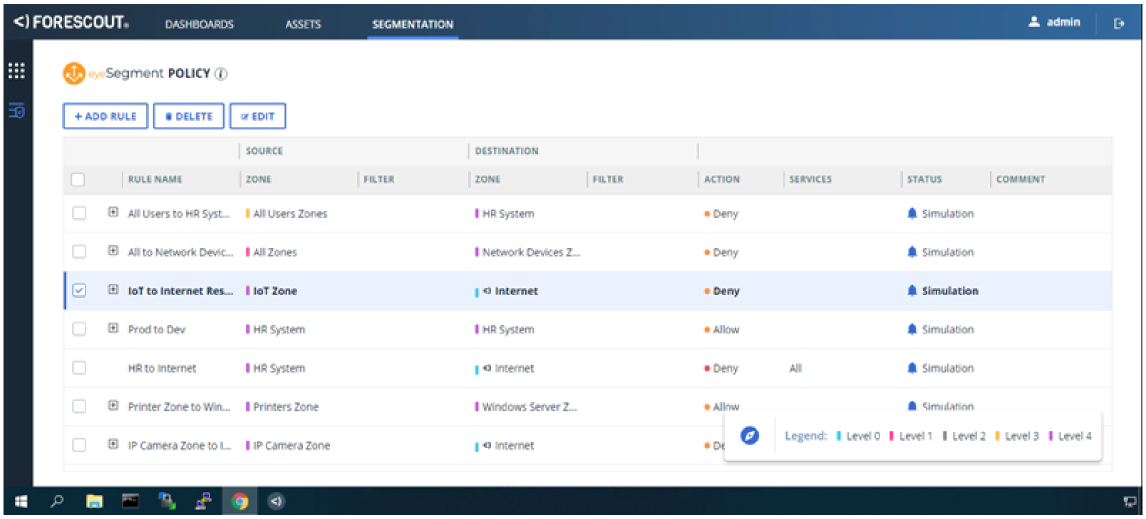
You are going to modify your eyeSegment policy to allow the NTP traffic from your printers to the Internet.

Step 1: Click **eyeSegment Policy** in the menu on the left of the page.



OCCURRENCES	STARTING FROM	LAST UPDATE
8.1k	Sun Mar 29 20:51:02	Mon Apr 06 08:06:04
8.1k	Sun Mar 29 20:51:02	Mon Apr 06 08:06:04

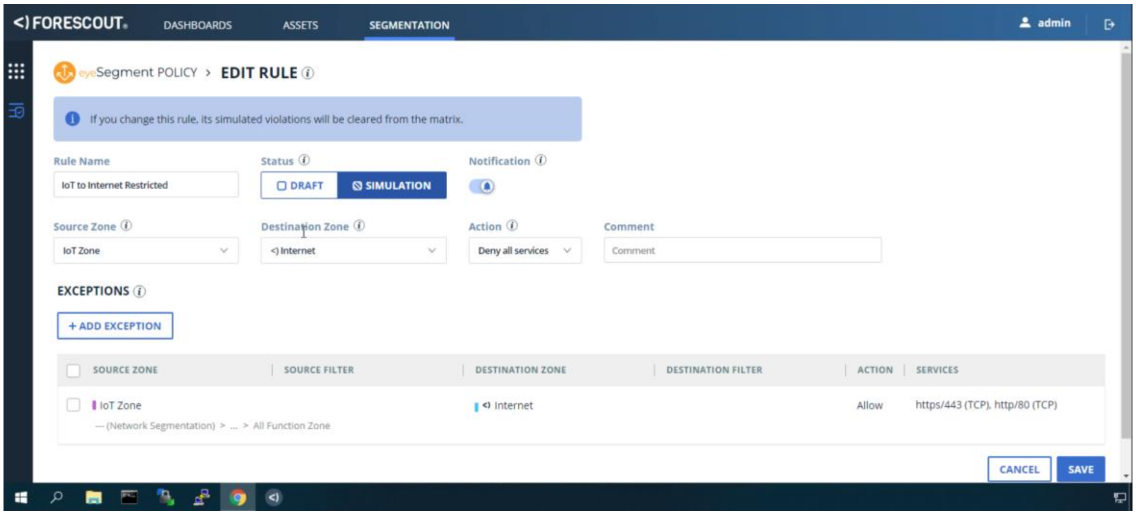
The list of policies you developed appears. You know that the Printers Zone is a subset of your IoT devices. There is already a rule for the IoT to Internet traffic. This is the rule you are going to modify.



		SOURCE		DESTINATION					
□	RULE NAME	ZONE	FILTER	ZONE	FILTER	ACTION	SERVICES	STATUS	COMMENT
□	⊞ All Users to HR Syst...	All Users Zones		HR System		Deny		Simulation	
□	⊞ All to Network Devic...	All Zones		Network Devices Z...		Deny		Simulation	
☑	⊞ **IoT to Internet Res...**	**IoT Zone**		**<) Internet**		**Deny**		**Simulation**	
□	⊞ Prod to Dev	HR System		HR System		Allow		Simulation	
□	HR to Internet	HR System		<) Internet		Deny	All	Simulation	
□	⊞ Printer Zone to Win...	Printers Zone		Windows Server Z...		Allow		Simulation	
□	⊞ IP Camera Zone to I...	IP Camera Zone		<) Internet		De			

Step 2: Select the checkbox next to the IoT to Internet and click **Edit**.

The eyeSegment policy editor appears. You are advised that the violations of rules being simulated will be cleared from the policy table. That is okay. Any new traffic that violates the modified policy will appear in the table.



eyeSegment POLICY > EDIT RULE

If you change this rule, its simulated violations will be cleared from the matrix.

Rule Name: IoT to Internet Restricted

Status: DRAFT [✓ SIMULATION]

Notification

Source Zone: IoT Zone

Destination Zone: Internet

Action: Deny all services

Comment: Comment

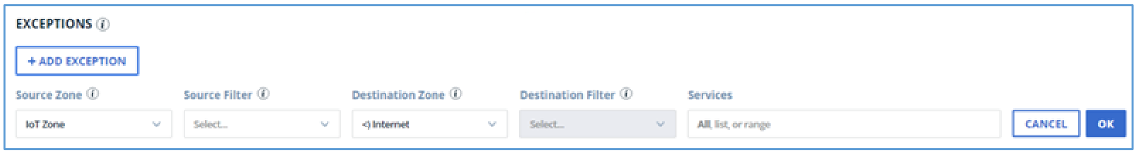
EXCEPTIONS

+ ADD EXCEPTION

□	SOURCE ZONE	SOURCE FILTER	DESTINATION ZONE	DESTINATION FILTER	ACTION	SERVICES
□	IoT Zone — (Network Segmentation) > ... > All Function Zone		Internet		Allow	https/443 (TCP), http/80 (TCP)

CANCEL SAVE

Step 3: Click **Add Exception**.



EXCEPTIONS

+ ADD EXCEPTION

Source Zone: IoT Zone

Source Filter: Select...

Destination Zone: Internet

Destination Filter: Select...

Services: All, list, or range

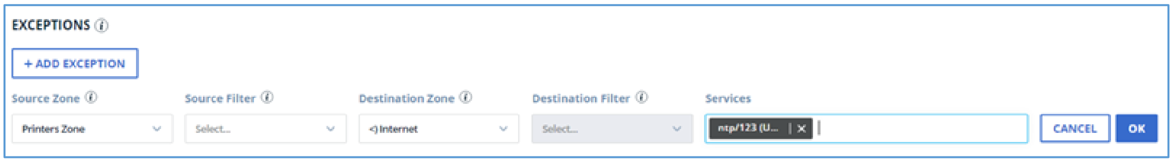
CANCEL OK

Step 4: Select **Printers Zone** from the **Source Zone** drop-down list.

Step 5: Keep the Source Filter field blank and leave the default value, Internet, in the Destination Zone.

Step 6: In the Services field, type NTP and then select **ntp/123 (UDP)**.

Your rule should look like this:



EXCEPTIONS

+ ADD EXCEPTION

Source Zone: Printers Zone

Source Filter: Select...

Destination Zone: Internet

Destination Filter: Select...

Services: ntp/123 (U... ×

CANCEL OK

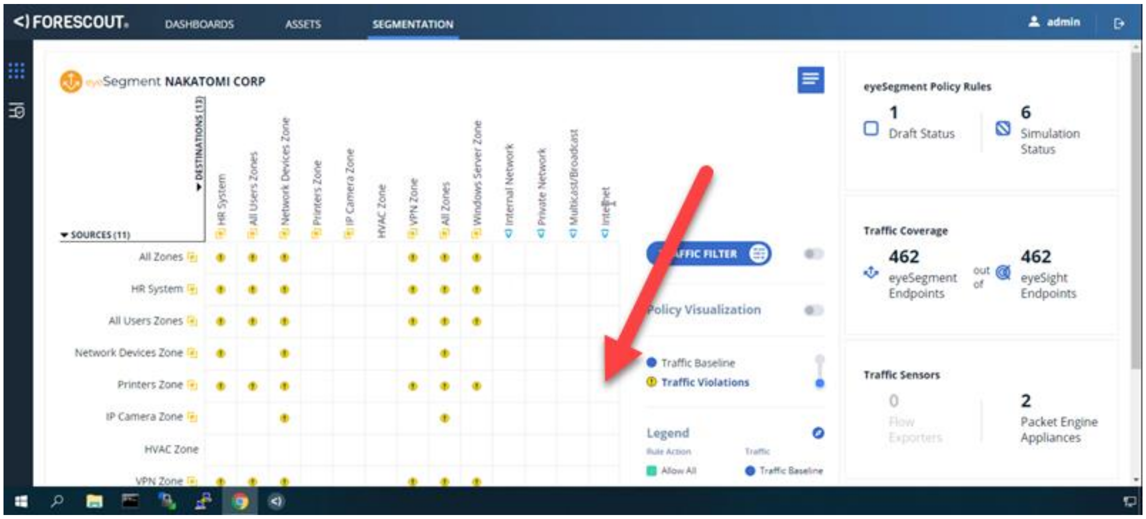
Step 7: Click OK.

The exception is added to the eyeSegment policy.

Step 8: Click **Save**.

Step 9: Click **eyeSegment Matrix** in the menu to the left.

Notice that the traffic violation icon has been removed from the Printer Zone to the Internet cell. This is because you modified the policy.



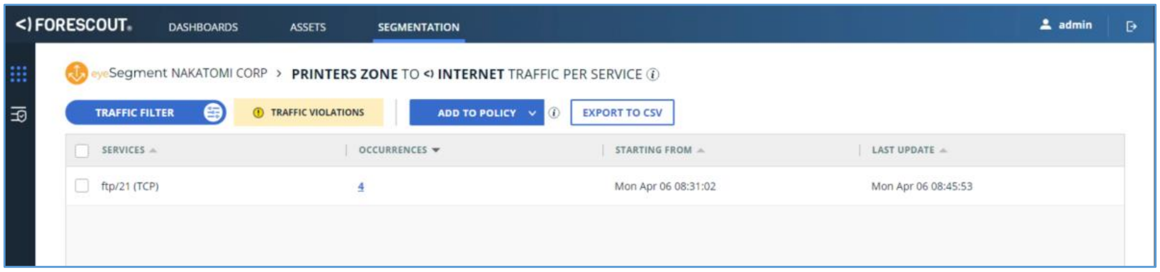
SOURCES (11) \ DESTINATIONS (13)	HR System	All Users Zones	Network Devices Zone	Printers Zone	IP Camera Zone	HVAC Zone	VPN Zone	All Zones	Windows Server Zone	Internal Network	Private Network	Multicast/Broadcast	Internet
All Zones	●	●	●				●	●	●				
HR System	●	●	●				●	●	●				
All Users Zones	●	●	●				●	●	●				
Network Devices Zone	●		●					●					
Printers Zone	●	●	●				●	●	●				
IP Camera Zone			●					●					
HVAC Zone													
VPN Zone	●	●	●				●	●	●				

eyeSegment Policy Rules
1 Draft Status
6 Simulation Status

Traffic Coverage
462 eyeSegment Endpoints out of 462 eyeSight Endpoints

Traffic Sensors
0 Flow Exporters
2 Packet Engine Appliances

The next time that the printers try to communicate to the Internet using FTP, you will see a violation in this cell. If you come back to this screen later, you will see a traffic violation. Drilling down on it will now show only the FTP traffic as a violation.



eyeSegment NAKATOMI CORP > PRINTERS ZONE TO INTERNET TRAFFIC PER SERVICE

SERVICES	OCCURRENCES	STARTING FROM	LAST UPDATE
ftp/21 (TCP)	4	Mon Apr 06 08:31:02	Mon Apr 06 08:45:53

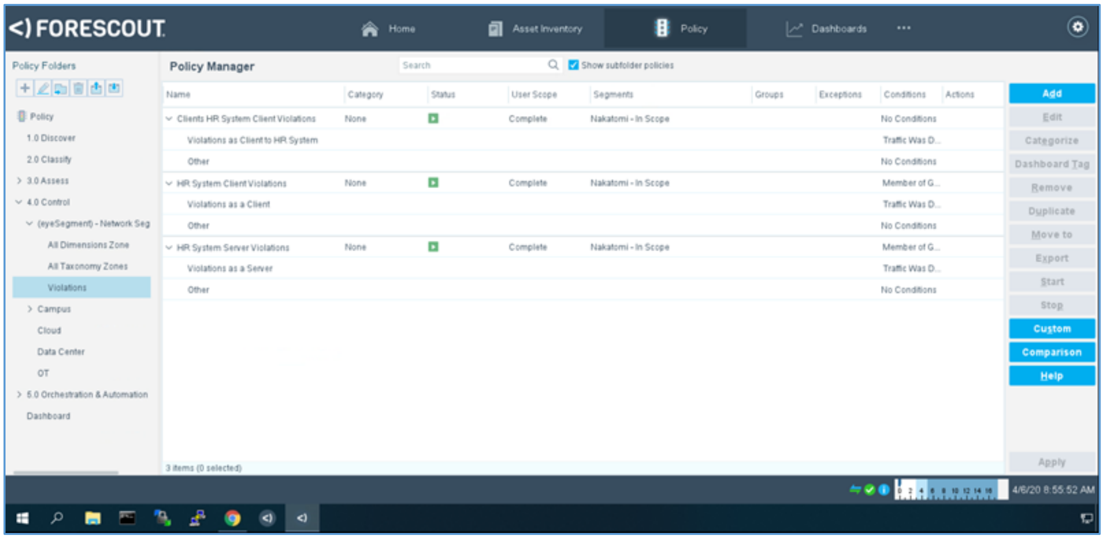
Next, you will build a policy in the Forescout console to handle the traffic violations.

Task 4: Create an eyeControl Policy to Address the Traffic Violations

Now that you have identified and simulated the traffic violations, it is time to act. You will use eyeControl to enforce your segmentation policies.

Step 1: Switch back to the Forescout console. Click the **Policy** tab.

Step 2: Expand the Policy tree: **Policy > 4.0 Control > (eyeSegment) Network Segmentation** and click **Violations**.



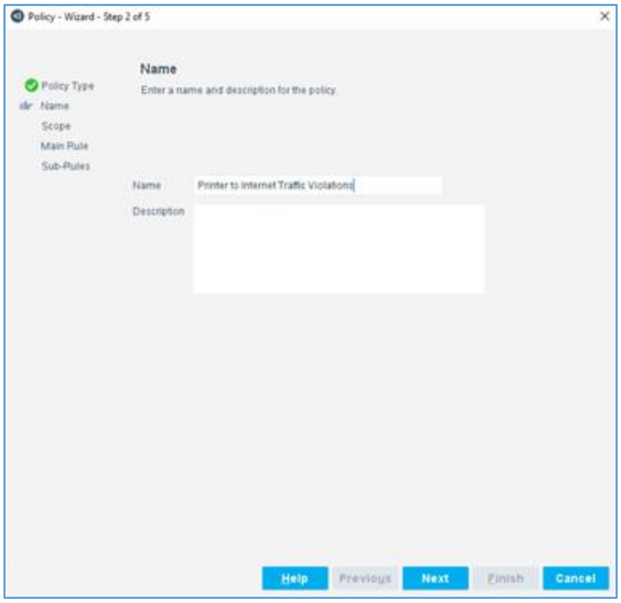
Name	Category	Status	User Scope	Segments	Groups	Exceptions	Conditions	Actions
Clients HR System Client Violations	None	▶	Complete	Nakatomi - In Scope			No Conditions	
Violations as Client to HR System							Traffic Was D...	
Other							No Conditions	
HR System Client Violations	None	▶	Complete	Nakatomi - In Scope			Member of G...	
Violations as a Client							Traffic Was D...	
Other							No Conditions	
HR System Server Violations	None	▶	Complete	Nakatomi - In Scope			Member of G...	
Violations as a Server							Traffic Was D...	
Other							No Conditions	

3 items (0 selected)

Step 3: Click **Add**.

The policy rule wizard appears. You will use a template to create this policy. Although you could use a policy template, you are going to create this policy from scratch.

Step 4: Click **Custom** at the bottom of the template list and then click **Next**.



Name

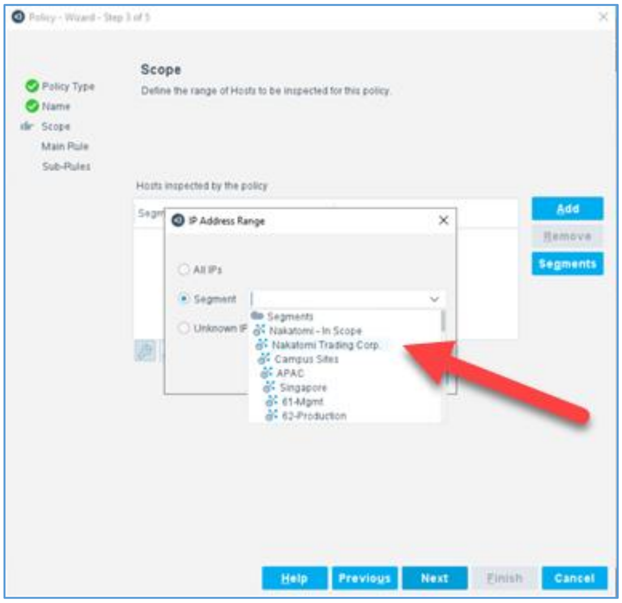
Enter a name and description for the policy.

Name: Printer to Internet Traffic Violations

Description:

Step 5: Type **Printer to Internet Traffic Violations** in the Name field. You can also add a description. Click **Next**.

The Scope dialog appears.



Scope

Define the range of Hosts to be inspected for this policy.

Hosts inspected by the policy

○ All IPs

● Segment

○ Unknown IP

Step 6: In the IP Address Range dialog, select **Nakatomi Trading Corp.** from the **Segment** drop-down list and click **OK**. Click **Next** to continue.

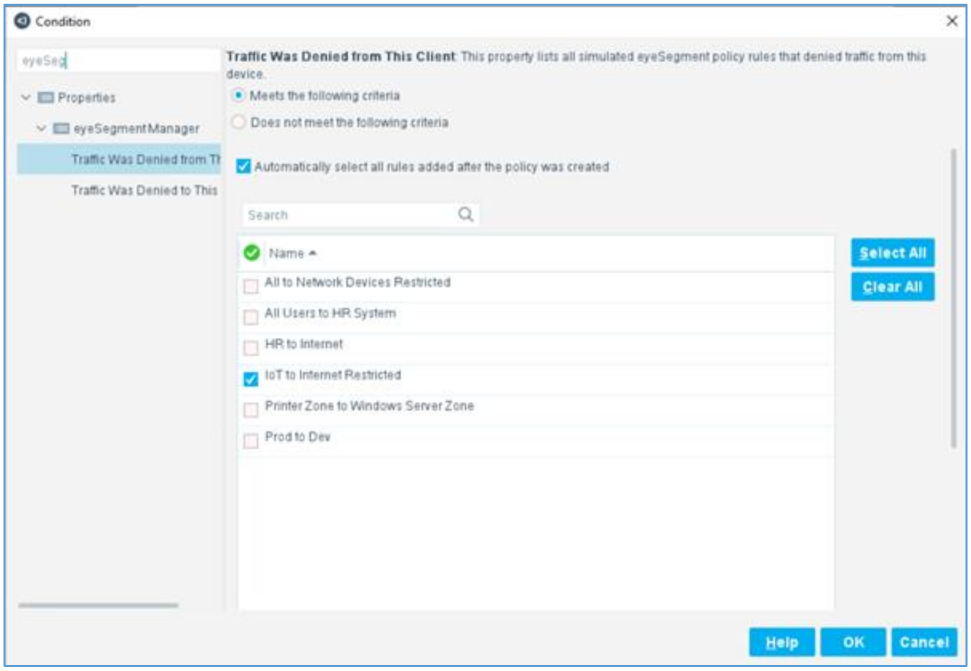
The Main Rule page appears.

Step 7: Create the Condition:

a. Click **Add** in the Condition area

The Condition dialog appears.

b. Type **eyeSegment** in the search field and click **Traffic Was Denied From This Client**.



Condition

eyeSeg

Properties
- eyeSegmentManager
  - Traffic Was Denied from Th
  - Traffic Was Denied to This

Traffic Was Denied from This Client This property lists all simulated eyeSegment policy rules that denied traffic from this device.

● Meets the following criteria

○ Does not meet the following criteria

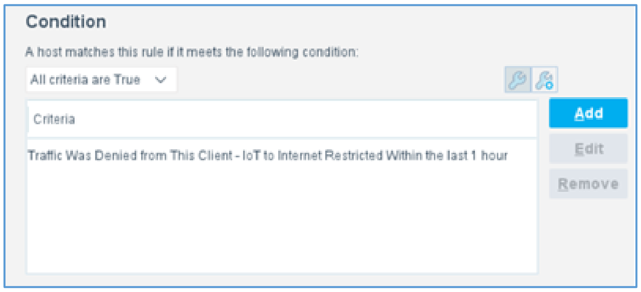
☑ Automatically select all rules added after the policy was created

Search

	Name
□	All to Network Devices Restricted
□	All Users to HR System
□	HR to Internet
☑	IoT to Internet Restricted
□	Printer Zone to Windows Server Zone
□	Prod to Dev

c. Select **IoT to Internet Restricted** and click **OK**.

The condition is added to the policy.



Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
Traffic Was Denied from This Client - IoT to Internet Restricted Within the last 1 hour

Remember, that was the eyeSegment policy that we modified to allow NTP but still deny FTP traffic.

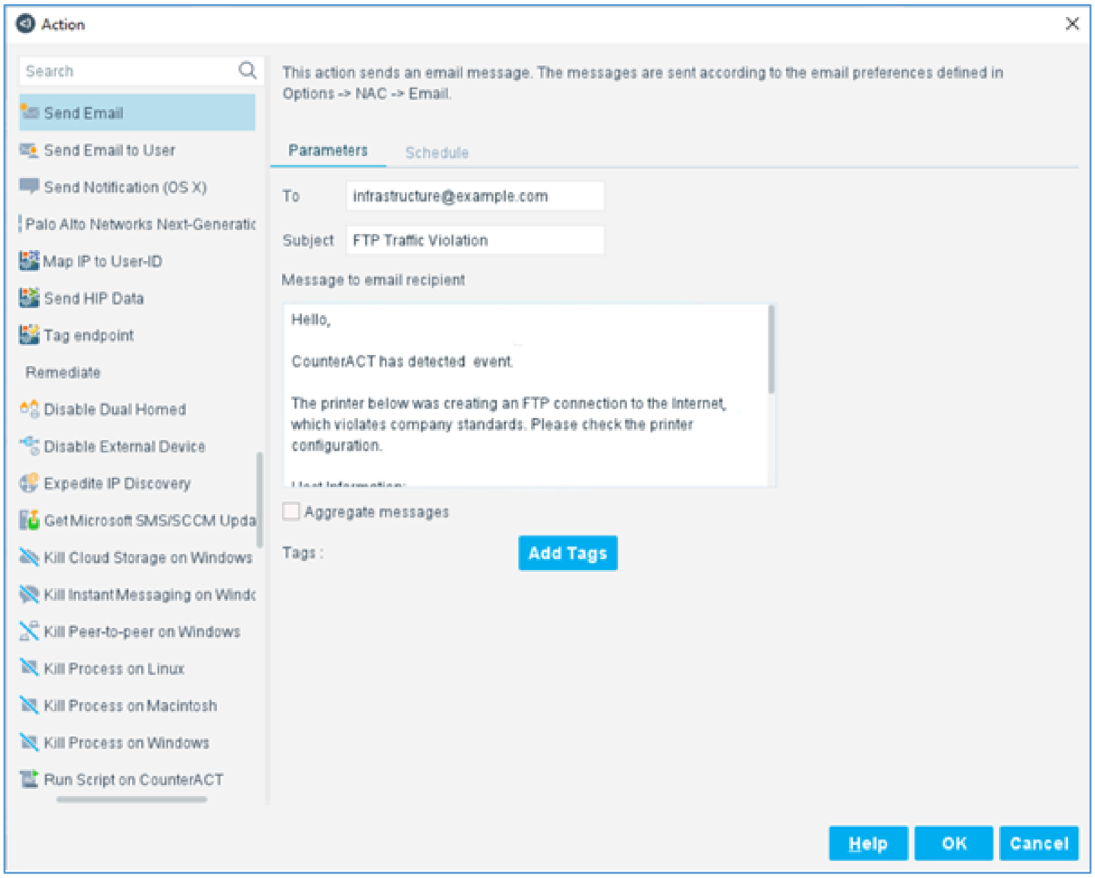
Step 8: Create the Action for this policy:

a. Click Add in the Actions area.

The Action dialog appears.

b. Expand the **Notify** folder and click **Send Email**.

We could take a variety of actions on the endpoints that violate the eyeSegment rule. We could block the endpoint from the network, block the specific traffic, create an incident report in our ticketing system, and more. For this exercise, we are simply going to send an email.



This action sends an email message. The messages are sent according to the email preferences defined in Options -> NAC -> Email.

To: infrastructure@example.com

Subject: FTP Traffic Violation

Message to email recipient

Hello,

CounterACT has detected event.

The printer below was creating an FTP connection to the Internet, which violates company standards. Please check the printer configuration.

Host Information:

□ Aggregate messages

Tags :

c. Change the following values:

To:	infrastructure@example.com (or, use your own email address)
Subject:	FTP Traffic Violation
Message	Add a bit more description above the Host Information, such as “The printer below was creating an FTP connection to the Internet, which violates company standards. Please check the printer configuration.”

d. Click **OK**.

The Action is added to your policy.

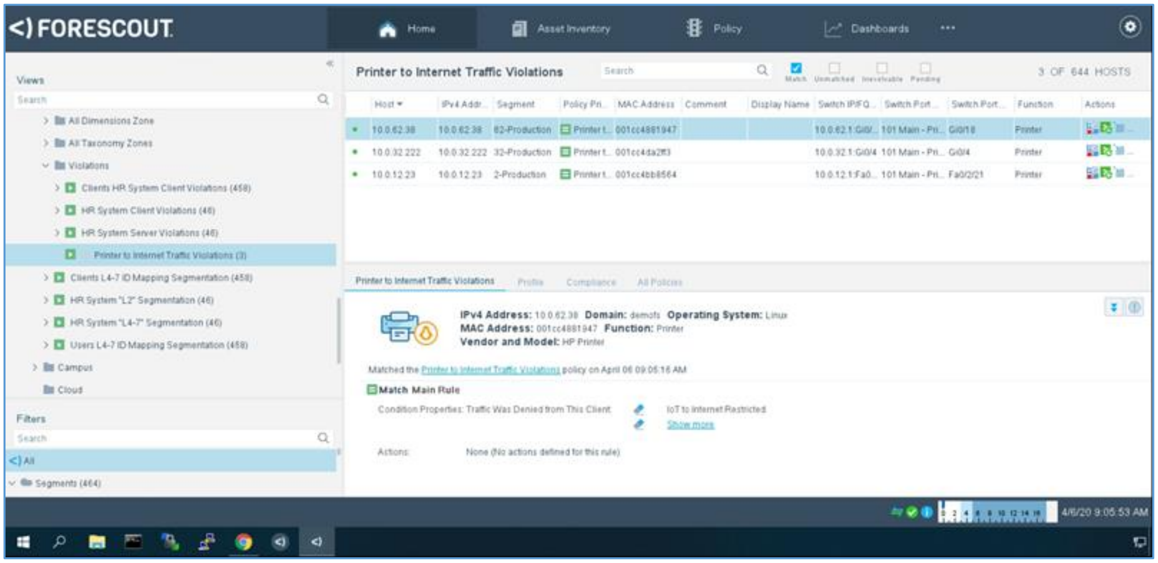
Step 9: Uncheck the **Enable** checkbox next to your action.

This is to prevent the system from actually sending email messages for each violation. If you added your own email address, you can leave it checked to see the results of your policy.

Step 10: Click **OK** to save the policy, and then click **Apply** to activate the policy.

Step 11: Click the **Home** tab and expand the policy tree: **Policies > 4.0 Control > (eyeSegment) – Network Segmentation > Violations**. Click **the Printer to Internet Traffic Violations** policy.

You can see the devices that have violated the rule you modified in eyeSegment.


FORESCOUT
Home
Asset Inventory
Policy
Dashboards
Views
Search
All Dimensions Zone
All Taxonomy Zones
Violations
Clients HR System Client Violations (458)
HR System Client Violations (46)
HR System Server Violations (46)
Printer to Internet Traffic Violations (3)
Clients L4-7 ID Mapping Segmentation (458)
HR System "L2" Segmentation (46)
HR System "L4-7" Segmentation (46)
Users L4-7 ID Mapping Segmentation (458)
Campus
Cloud
Filters
Search
All
Segments (464)
Search
Match
Unmatched
Irresolvable
Pending
Profile
Compliance
All Policies
Show more

Printer to Internet Traffic Violations — ☑ Match □ Unmatched □ Irresolvable □ Pending — 3 OF 644 HOSTS

	Host	IPv4 Addr...	Segment	Policy Pri...	MAC Address	Comment	Display Name	Switch IP/FQ...	Switch Port...	Switch Port...	Function
●	10.0.62.38	10.0.62.38	62-Production	Printer t...	001cc4881947			10.0.62.1:Gi0/...	101 Main - Pri...	Gi0/18	Printer
●	10.0.32.222	10.0.32.222	32-Production	Printer t...	001cc4da2ff3			10.0.32.1:Gi0/4	101 Main - Pri...	Gi0/4	Printer
●	10.0.12.23	10.0.12.23	2-Production	Printer t...	001cc4bb8564			10.0.12.1:Fa0...	101 Main - Pri...	Fa0/2/21	Printer

Printer to Internet Traffic Violations

IPv4 Address: 10.0.62.38 **Domain:** demofs **Operating System:** Linux
MAC Address: 001cc4881947 **Function:** Printer
Vendor and Model: HP Printer

Matched the Printer to Internet Traffic Violations policy on April 06 09:05:16 AM

Match Main Rule

Condition Properties: Traffic Was Denied from This Client — IoT to Internet Restricted

Actions: None (No actions defined for this rule)

4/6/20 9:05:53 AM

Follow Up

- Do you currently have any segmentation projects? Could eyeSegment hep you accelerate those projects? Reduce the risk of downtime?
- Do you currently have specific situations where eyeSegment could help you reduce your attack surface?
- Do you have any gaps in knowing which of your devices are talking to others? To the Internet? How do you currently keep track of that information? How are you notified when violation to your corporate policy occur?

Take the Next Step

Learn more about how you can drive your security initiatives forward using the Forescout platform. We offer several complimentary options to further boost your knowledge, help engage your peers and share the business benefits of agentless visibility, policy-based control and multivendor security orchestration.

- **Spend 10 minutes with the Forescout Business Value ROI Tool**. This tool, based on IDC's methodology, provides statistical analysis of the business impact the Forescout platform can deliver to your organization. It generates a custom ROI report that you can share with co-workers.
- **Visit forescout.com for more information**, including details on our growing list of Forescout products that share device context between the Forescout platform and many of the security and IT management tools you use today. Forescout eyeExtend modules can help automate policy enforcement across disparate solutions, accelerate system-wide response to mitigate risks and increase productivity in multiple ways.
- **Contact Forescout to set up an appointment:**
  salesdev@forescout.com
  Tel: +1-866-329-9352