A SANS Product Review

Device Visibility and Control: Streamlining IT and OT Security with Forescout

Written by **Don Murdoch**

August 2019

Sponsored by:

Forescout

Introduction

Device visibility remains a daunting challenge for the modern enterprise. Forescout provides a multifaceted information technology (IT) and operational technology (OT) platform designed to solve visibility challenges for the modern enterprise by providing complete device discovery and classification, risk assessment, compliance, orchestration and automated security controls.

Forescout's latest release[1] significantly extends the platform's long-standing reputation for network admission controls and device visibility. In addition to deep device visibility in IT environments, the updated platform uses passive analysis to assess devices at all layers of the OT network, as outlined in the Purdue Enterprise Reference Architecture model.[2] Passive analysis is particularly important in terms of ensuring safety and avoiding disruption of critical services in OT and medical device networks, given the business processes those networks and devices support.

Gartner has recently stated that CIOs and IT leaders who understand the need for higher levels of IT and OT integration and awareness will reach critical mass by 2020.[3] The research firm further predicts that IoT will significantly impact the overall economy, support numerous business process use cases, lead to cost savings for some sectors

[1] SANS investigated version 8.1 of the Forescout platform for this review.

[2] "Purdue Reference Model for CIM," www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

[3] "Leading the IoT: Gartner Insights on How to Lead in a Connected World," www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

and represent a significant component to solution-level thinking. Therefore, increased usage of IoT on the enterprise network presents an increased need for device visibility, which Forescout satisfies.

In line with that expectation, we've identified six key questions facing modern enterprises and IT leaders:

- What devices are on the network? IT must have a full inventory of all IT, IoT, cloud, data center and OT assets accessing the network.
- How can IT gather and maintain relevant information about any device on the network in order to implement asset management practices?
- How can organizations detect and respond to unknown, insecure or vulnerable devices?
- Once a device gains network permission, how can IT provide assurance that IT, OT and IoT devices are operating to the organization's security standards?
- How does IT minimize staffing requirements while maintaining the security state in various IT systems, even when adverse device conditions occur?
- Aside from campus and OT networks, how are these questions answered in data center and cloud environments?

This paper will answer these (and other) questions and discuss five major product features of the Forescout platform.

Considering the statistics highlighted in the "SANS Research" sidebar, it is clear why device visibility is such a hot topic. Forescout tackles the requirements of modern enterprises and IT leaders who need to empower their teams and want to get ahead of the proliferation of network-aware devices—providing insight into device discovery, auto-classification of endpoints, risk and posture assessment, automated security controls, and scalability and flexibility. This SANS review answers the key questions as it investigates the core capabilities of the Forescout platform, considering each in the context of the needs of IT, OT and security professionals.

SANS Research

SANS Institute's own surveys reveal how organizations suffer when it comes to device visibility, corroborating the concerns raised in the six key questions.

The 296 respondents to the 2018 SANS SOC Survey[4] indicated that full inventories are lacking:

- Only 19 of 296 respondents (6%) had a 100% device and endpoint inventory.
- 103 respondents (35%) had a 76% to 99% inventory.
- 174 respondents (59%) had less than 75% inventory.

The 2018 SANS Industrial IoT Security Survey[5] reveals rapid growth in IoT devices, a significant portion of which do not follow the Purdue model:

- Most organizations envision 10% to 25% growth in their connected devices for the foreseeable future.
- A further 32% of IoT devices connect directly to the Internet, thus bypassing traditional security layers as referenced in the Purdue model, which presents a significant risk should an IoT device suffer a compromise.

[4] "The Definition of SOC-cess? SANS 2018 Security Operations Center Survey," August 2018, www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018-security-operations-center-survey-38570

[5] "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," July 2018, www.sans.org/reading-room/whitepapers/analyst/2018-industrial-iot-security-survey-shaping-iiot-security-concerns-38505

Solving Real-World Problems with Real-World Value

In our review of the Forescout platform, it was easy to see the larger tapestry against which Forescout could be a useful tool to counter threats to the organization. While there are multiple scenarios in which Forescout would be an asset, we investigated four specific instances the author has encountered firsthand:

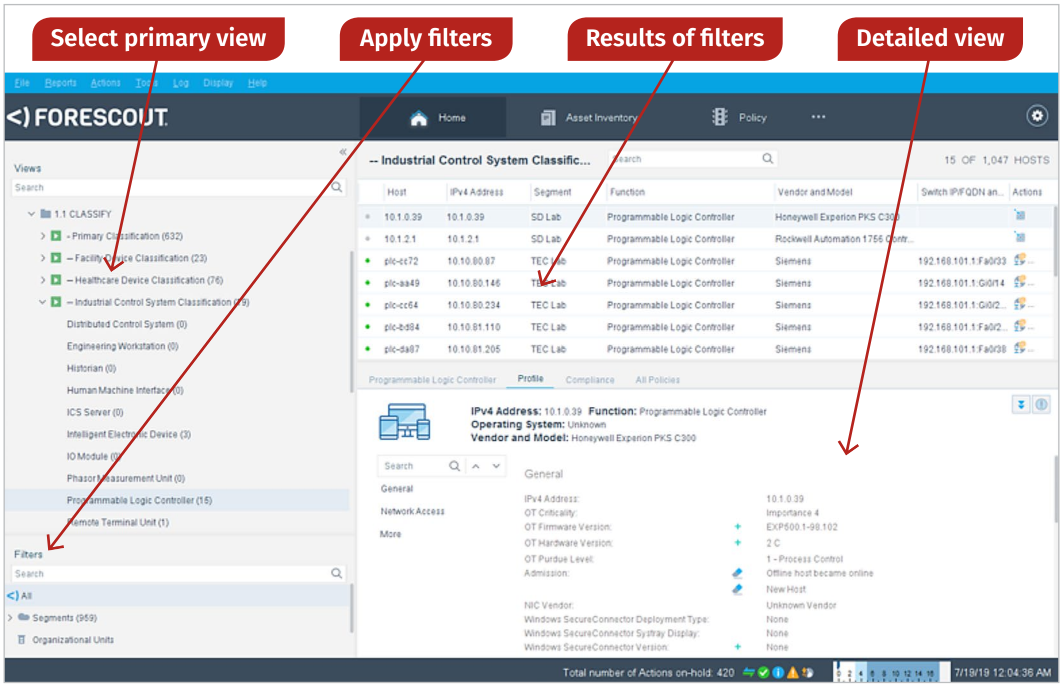
- **Inability to discover and classify assets networkwide—**Without a well-maintained configuration management database (CMDB), it is incredibly difficult to have an accurate networkwide view that can be both searched by analysts and consumed in a downstream, data-dependent system like a SIEM tool. When a SIEM system receives metadata (such as name, owner, CVE and location), it can use that metadata when processing other event data to generate an alert. When data in the CMDB is also present in the SIEM system, analysts have a significantly lower click rate because they don't have to look up data in many different systems. Forescout can help consolidate the real-time view of assets for integration or import, thanks to its ability to discover and provide in-depth context for devices across all environments—the campus, data center, OT networks, AWS and Azure cloud, and VMware—and supply a single view of organization-wide assets. This capability is integral to providing the level of asset awareness that security operations centers (SOCs) need when reviewing alerts.
- **Users with elevated access (local admin) disabling security tools—**It is common to have users with admin rights turning off a security tool in response to a real or perceived issue. Forescout, through its automation features, re-enables security tools to maintain device compliance and provide a notification to security admins who can then resolve the issue and fine-tune the settings.
- **Users connecting unauthorized devices to the LAN—**Vendors, external auditors, temp workers and others routinely connect to corporate networks with non-corporate computers, digital media devices using peer-to-peer networking, unauthorized wireless access points or even small computers the size of a deck of cards with a "security" distribution installed. Regardless of the source, organizations face considerable risk from unauthorized devices accessing the network via a wired connection. Forescout can be configured to identify rogue devices, even if the user has cloned the MAC address of an authorized device such as a rarely used PC that will not be noticed for several days.
- **Scattered infrastructure staff and numerous systems—**It is not uncommon for incident responders to consult half a dozen different infrastructure systems and staff to gather various data in response to a single threat incident. Forescout streamlines data collection processes by providing a single focal point for device data. It organizes a significant amount of observed and collected data about an endpoint as it connects to and uses network resources. Examples include port/switch information, network-accessible services, user data, recently running processes and services, and vulnerability data.

Improving Visibility Through an Efficient Interface

The Forescout platform provides a wealth of endpoint device discovery and visibility options, and it does so through a highly unified interface that follows a natural flow from left to right. Forescout's primary console is so well-designed that one can get the impression that the system is "simple"—even though its capabilities and features are deep and rich.

Interface Simplified

The user interface is designed to provide the information needed expediently. Forescout's primary console provides tools that reflect what the user actually does, keeps things simple, is consistent, maintains high utility and is arranged to make it very easy to locate endpoint data. For example, the upper section of the left panel selects the primary view and the lower section applies filters, as needed (see Figure 1).


Select primary view
Apply filters
Results of filters
Detailed view
File
Reports
Actions
Tools
Log
Display
Help
<) FORESCOUT
Home
Asset Inventory
Policy
•••
Views
Search
1.1 CLASSIFY
- Primary Classification (632)
– Facility Device Classification (23)
– Healthcare Device Classification (76)
– Industrial Control System Classification (19)
Distributed Control System (0)
Engineering Workstation (0)
Historian (0)
Human Machine Interface (0)
ICS Server (0)
Intelligent Electronic Device (3)
IO Module (0)
Phasor Measurement Unit (0)
Programmable Logic Controller (15)
Remote Terminal Unit (1)
Filters
Search
<) All
Segments (959)
Organizational Units
-- Industrial Control System Classific...
Search
15 OF 1,047 HOSTS
Programmable Logic Controller
Profile
Compliance
All Policies
Search
General
Network Access
More
Total number of Actions on-hold: 420
7/19/19 12:04:36 AM

Host	IPv4 Address	Segment	Function	Vendor and Model	Switch IP/FQDN an...	Actions
10.1.0.39	10.1.0.39	SD Lab	Programmable Logic Controller	Honeywell Experion PKS C300		
10.1.2.1	10.1.2.1	SD Lab	Programmable Logic Controller	Rockwell Automation 1756 Contr...		
plc-cc72	10.10.80.87	TEC Lab	Programmable Logic Controller	Siemens	192.168.101.1:Fa0/33	
plc-aa49	10.10.80.146	TEC Lab	Programmable Logic Controller	Siemens	192.168.101.1:Gi0/14	
plc-cc64	10.10.80.234	TEC Lab	Programmable Logic Controller	Siemens	192.168.101.1:Gi0/2...	
plc-bd84	10.10.81.110	TEC Lab	Programmable Logic Controller	Siemens	192.168.101.1:Fa0/2...	
plc-da87	10.10.81.205	TEC Lab	Programmable Logic Controller	Siemens	192.168.101.1:Fa0/38	

IPv4 Address: 10.1.0.39 **Function:** Programmable Logic Controller
Operating System: Unknown
Vendor and Model: Honeywell Experion PKS C300

General

IPv4 Address:	10.1.0.39
OT Criticality:	Importance 4
OT Firmware Version:	EXP600.1-98.102
OT Hardware Version:	2.C
OT Purdue Level:	1 - Process Control
Admission:	Offline host became online
	New Host
NIC Vendor:	Unknown Vendor
Windows SecureConnector Deployment Type:	None
Windows SecureConnector Systray Display:	None
Windows SecureConnector Version:	None

Figure 1. Asset and Host Details on the Easy-to-Navigate Forescout Console

As the user applies views and filters, the results are updated in the upper primary view and are responsive to the tab selected (home, asset inventory or policy). The full details of a selected device appear in the Host Details pane. Last, each of the three navigation views has its own search capability, a handy feature that simplifies investigations.

New to the latest iteration of Forescout is a customizable dashboard. An analyst can configure a dashboard to provide a consolidated view of the entire device landscape across all environments or tune the dashboard to provide a view for the security operations team. See Figure 2 for an example of the detail the dashboard shows.

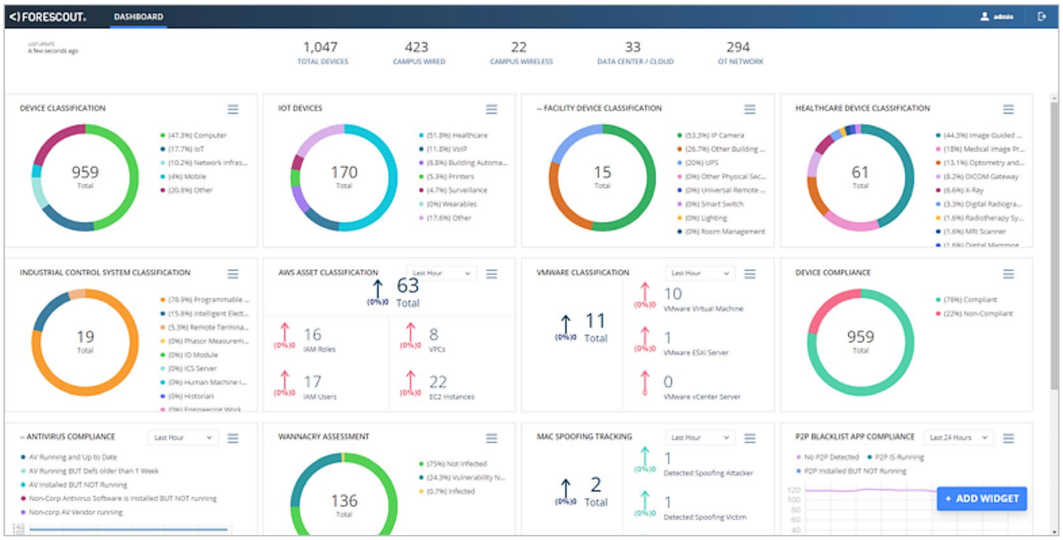


Figure 2. Dashboard's Customized Views of Network-Connected Devices

Device Discovery Options

Forescout features a variety of device discovery options, offering detailed visibility to the endpoints connected to the network—be they on premises, in the data center or in the cloud. The options include learning from existing network sources and full-traffic monitoring. These methods use passive network discovery, which collects data about endpoints as they come onto the network (also referred to as *admission events*).

Full-traffic monitoring is attained by actively monitoring traffic from a device through network extraction of data provided by a SPAN/mirror port or a TAP.

Forescout's different passive and active techniques play a key role in enabling customers to gain 100% device discovery and visibility without having to redesign the network or deploy additional hardware.

Passive Network Device Discovery

Forescout leverages a wide variety of techniques to passively identify endpoints with minimum network intrusion or reconfiguration. For medical, ICS, SCADA and other OT networks, the ability to passively identify assets with no network change or disruption is critical, to avoid impacting the line process.

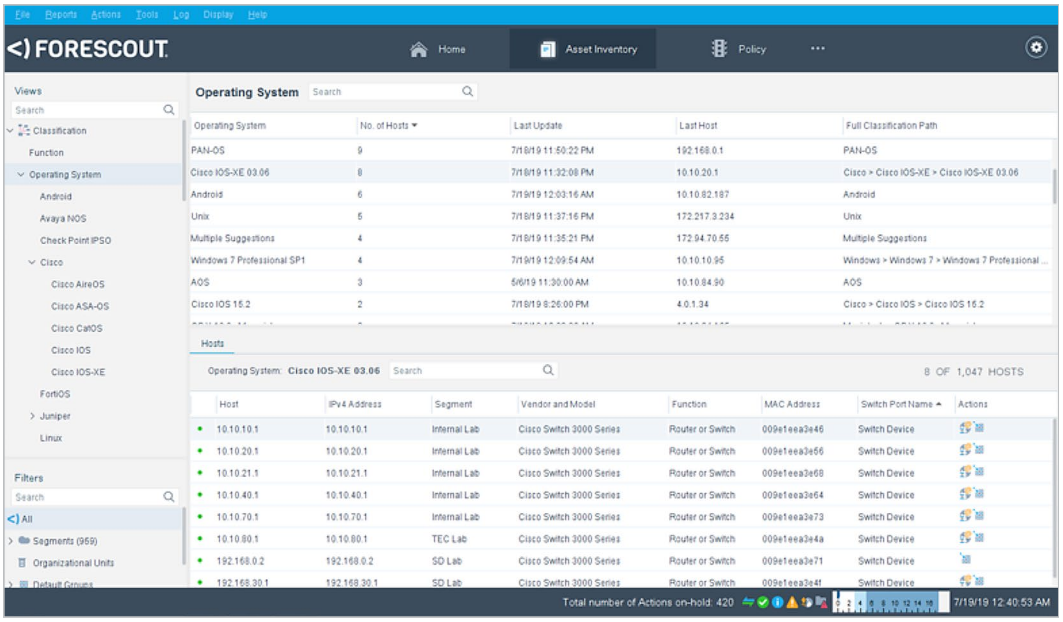
Passive discovery methods include monitoring DHCP leases, receiving SNMP traps from dozens of network device manufacturers, monitoring RADIUS connections, receiving NetFlow data, polling network infrastructure devices and wireless controllers, querying a CMDB and traffic monitoring via SPAN. Flow data can also be used to profile systems because traffic flow can help define a device's function. These techniques all occur "naturally," and Forescout's structure leverages all of those events. Forescout also supports discovery for data center and cloud environments through API integrations.

Active Profiling and Rogue Device Detection

In contrast to passive techniques, Forescout's active techniques use both network and device querying. Each of these feature sets can be enabled on a segment-by-segment basis. That way, at the initial network connection event, the platform can prompt non-corporate users to authenticate over a captive web portal, which in turn means they can authenticate against a variety of different authentication stores and establish user identity at the very beginning of a network connection.

The benefit of this technique is that Forescout maintains the "user to IP to MAC address" correlation as endpoints arrive on the network. The obvious attack vector is to clone and then attempt to reuse an authorized device's MAC address. Because Forescout is the LAN and WLAN gatekeeper, when the cloned MAC address connects to the network, Forescout immediately detects the spoofing event and can take appropriate actions to block the attacker.

On initial network connection and periodically thereafter, Forescout also collects an inventory of installed applications, packages, vulnerabilities and system compliance states via remote Windows Management Instrumentation (WMI), remote procedure calls and SSH. The system will also query switches every 60 seconds so that it has visibility into OSI Layer 2 for the enterprise.



Operating System

Operating System	No. of Hosts	Last Update	Last Host	Full Classification Path
PAN-OS	9	7/18/19 11:50:22 PM	192.168.0.1	PAN-OS
Cisco IOS-XE 03.06	8	7/18/19 11:32:08 PM	10.10.20.1	Cisco > Cisco IOS-XE > Cisco IOS-XE 03.06
Android	6	7/19/19 12:03:16 AM	10.10.82.187	Android
Unix	5	7/18/19 11:37:16 PM	172.217.3.234	Unix
Multiple Suggestions	4	7/18/19 11:35:21 PM	172.94.70.55	Multiple Suggestions
Windows 7 Professional SP1	4	7/19/19 12:09:54 AM	10.10.10.95	Windows > Windows 7 > Windows 7 Professional ...
AOS	3	5/6/19 11:30:00 AM	10.10.84.90	AOS
Cisco IOS 15.2	2	7/18/19 8:26:00 PM	4.0.1.34	Cisco > Cisco IOS > Cisco IOS 15.2

Operating System: **Cisco IOS-XE 03.06** 8 OF 1,047 HOSTS

Host	IPv4 Address	Segment	Vendor and Model	Function	MAC Address	Switch Port Name	Actions
10.10.10.1	10.10.10.1	Internal Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e46	Switch Device	
10.10.20.1	10.10.20.1	Internal Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e56	Switch Device	
10.10.21.1	10.10.21.1	Internal Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e68	Switch Device	
10.10.40.1	10.10.40.1	Internal Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e64	Switch Device	
10.10.70.1	10.10.70.1	Internal Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e73	Switch Device	
10.10.80.1	10.10.80.1	TEC Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e4a	Switch Device	
192.168.0.2	192.168.0.2	SD Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e71	Switch Device	
192.168.30.1	192.168.30.1	SD Lab	Cisco Switch 3000 Series	Router or Switch	009e1eea3e4f	Switch Device	

Total number of Actions on-hold: 420 7/19/19 12:40:53 AM

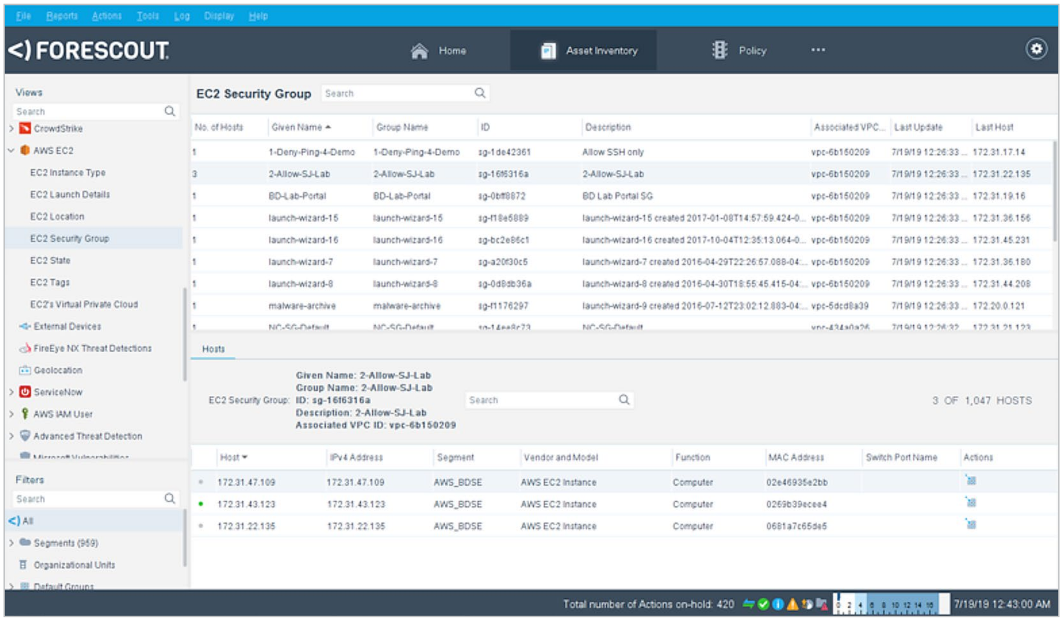
Figure 3. OS Visibility Based on Detected Properties

The platform has a variety of active service and software discovery capabilities. At the lowest level, the system can run the well-known **nmap** scanning tool to fingerprint the IP stack and operating system (see Figure 3).

Data Center and Cloud Asset Inventory

Forescout queries specific cloud systems through API calls enabled through a plug-in module, like many other cloud integrations today. This enables cloud asset inventories to be displayed together with local asset inventory.

For AWS, the platform retrieves Elastic Compute Cloud (EC2) instance or endpoint configuration information, identity access management users and virtual private cloud configuration information. The platform also detects Elastic Block Store (EBS) encryption status. The AWS plug-in can be set up for read access to support visibility and read/write for control functions. Forescout has flexible policy settings to ensure cloud environments are maintained in accordance with the organization's security policies. For example, analysts can set policies to determine which security groups should be attached to EC2 instances. See Figure 4.



EC2 Security Group

No. of Hosts	Given Name	Group Name	ID	Description	Associated VPC...	Last Update	Last Host
1	1-Deny-Ping-4-Demo	1-Deny-Ping-4-Demo	sg-1de42361	Allow SSH only	vpc-6b150209	7/19/19 12:26:33 ...	172.31.17.14
3	2-Allow-SJ-Lab	2-Allow-SJ-Lab	sg-16f6316a	2-Allow-SJ-Lab	vpc-6b150209	7/19/19 12:26:33 ...	172.31.22.135
1	BD-Lab-Portal	BD-Lab-Portal	sg-0bff8872	BD Lab Portal SG	vpc-6b150209	7/19/19 12:26:33 ...	172.31.19.16
1	launch-wizard-15	launch-wizard-15	sg-f18e5889	launch-wizard-15 created 2017-01-08T14:57:59.424-0...	vpc-6b150209	7/19/19 12:26:33 ...	172.31.36.156
1	launch-wizard-16	launch-wizard-16	sg-bc2e86c1	launch-wizard-16 created 2017-10-04T12:35:13.064-0...	vpc-6b150209	7/19/19 12:26:33 ...	172.31.45.231
1	launch-wizard-7	launch-wizard-7	sg-a20f30c5	launch-wizard-7 created 2016-04-29T22:26:57.088-04:...	vpc-6b150209	7/19/19 12:26:33 ...	172.31.36.180
1	launch-wizard-8	launch-wizard-8	sg-0d8db36a	launch-wizard-8 created 2016-04-30T18:55:45.415-04:...	vpc-6b150209	7/19/19 12:26:33 ...	172.31.44.208
1	malware-archive	malware-archive	sg-f1176297	launch-wizard-9 created 2016-07-12T23:02:12.883-04:...	vpc-5dcd8a39	7/19/19 12:26:33 ...	172.20.0.121

EC2 Security Group: **Given Name: 2-Allow-SJ-Lab**
Group Name: 2-Allow-SJ-Lab
ID: sg-16f6316a
Description: 2-Allow-SJ-Lab
Associated VPC ID: vpc-6b150209

3 OF 1,047 HOSTS

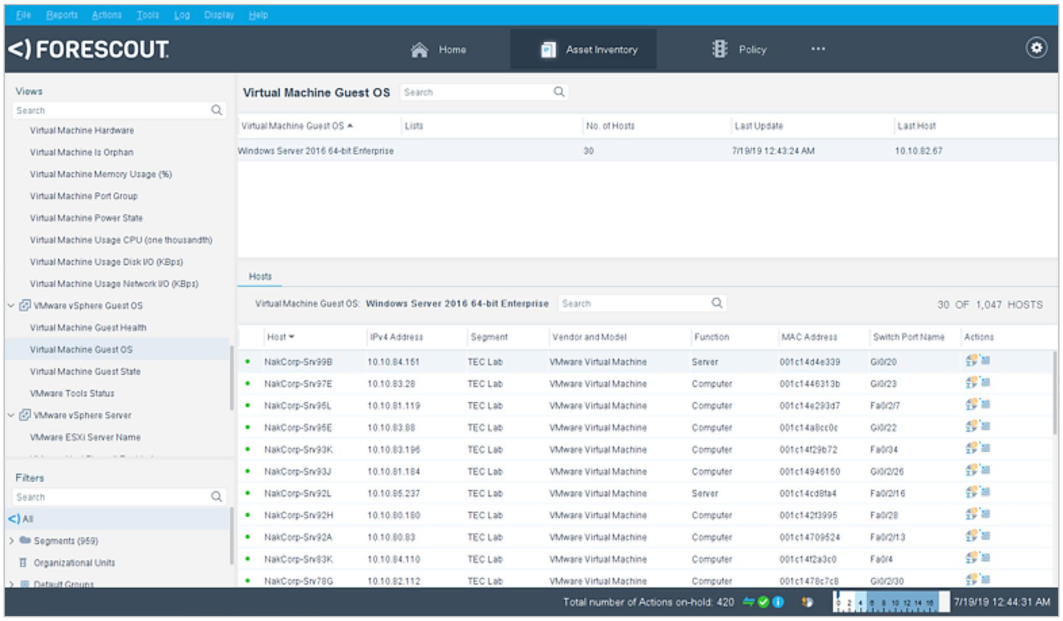
Host	IPv4 Address	Segment	Vendor and Model	Function	MAC Address	Switch Port Name	Actions
172.31.47.109	172.31.47.109	AWS_BDSE	AWS EC2 Instance	Computer	02e46935e2bb		
172.31.43.123	172.31.43.123	AWS_BDSE	AWS EC2 Instance	Computer	0269b39ecee4		
172.31.22.135	172.31.22.135	AWS_BDSE	AWS EC2 Instance	Computer	0681a7c65de5		

Total number of Actions on-hold: 420 7/19/19 12:43:00 AM

Figure 4. EC2 Hosts Shown in Descending Count Order, Arranged by AWS Security Groups

Forescout has similar capabilities for Azure. These capabilities bring cloud systems into a centralized asset awareness and management plane. It can read VM instances and VNets and monitor delete protection status.

For an on-premises cloud provided by VMware, Forescout retrieves highly granular VM host data and reads guest OS properties. VMware NSX, which is an integral part of VMware's software-defined data center strategy, can also be co-managed along with other data center and campus network segments. See Figure 5.



Virtual Machine Guest OS

Virtual Machine Guest OS	Lists	No. of Hosts	Last Update	Last Host
Windows Server 2016 64-bit Enterprise		30	7/19/19 12:43:24 AM	10.10.82.67

Virtual Machine Guest OS: **Windows Server 2016 64-bit Enterprise**

30 OF 1,047 HOSTS

	Host	IPv4 Address	Segment	Vendor and Model	Function	MAC Address	Switch Port Name	Actions
●	NakCorp-Srv99B	10.10.84.151	TEC Lab	VMware Virtual Machine	Server	001c14d4e339	Gi0/20	
●	NakCorp-Srv97E	10.10.83.28	TEC Lab	VMware Virtual Machine	Computer	001c1446313b	Gi0/23	
●	NakCorp-Srv95L	10.10.81.119	TEC Lab	VMware Virtual Machine	Computer	001c14e293d7	Fa0/2/7	
●	NakCorp-Srv95E	10.10.83.88	TEC Lab	VMware Virtual Machine	Computer	001c14a8cc0c	Gi0/22	
●	NakCorp-Srv93K	10.10.83.196	TEC Lab	VMware Virtual Machine	Computer	001c14f29b72	Fa0/34	
●	NakCorp-Srv93J	10.10.81.184	TEC Lab	VMware Virtual Machine	Computer	001c14946160	Gi0/2/26	
●	NakCorp-Srv92L	10.10.85.237	TEC Lab	VMware Virtual Machine	Server	001c14cd8fa4	Fa0/2/16	
●	NakCorp-Srv92H	10.10.80.180	TEC Lab	VMware Virtual Machine	Computer	001c142f3995	Fa0/28	
●	NakCorp-Srv92A	10.10.80.83	TEC Lab	VMware Virtual Machine	Computer	001c14709524	Fa0/2/13	
●	NakCorp-Srv83K	10.10.84.110	TEC Lab	VMware Virtual Machine	Computer	001c14f2a3c0	Fa0/4	
●	NakCorp-Srv78G	10.10.82.112	TEC Lab	VMware Virtual Machine	Computer	001c1478c7c8	Gi0/2/30	

Total number of Actions on-hold: 420

7/19/19 12:44:31 AM

Figure 5. An Example Showing Data from VMware

Without this single asset inventory plane provided by Forescout, analysts would have to extract data on an as-needed basis and manage a cobbled-together inventory, which would have to be painstakingly maintained by importing CSV data into Excel and struggling through unwieldy spreadsheet functions and vLookups across multiple tabs in order to resolve heterogeneous data into a consolidated asset view.

Classification and Asset Management

Once devices are discovered on the network, Forescout automatically classifies them by mapping device properties against a library of thousands of device profiles. The result is an inventory of devices that is searchable based on asset categories. Forescout has dozens of functional categories, ranging from traditional IT devices and healthcare devices to enterprise IoT and ICS/OT devices.

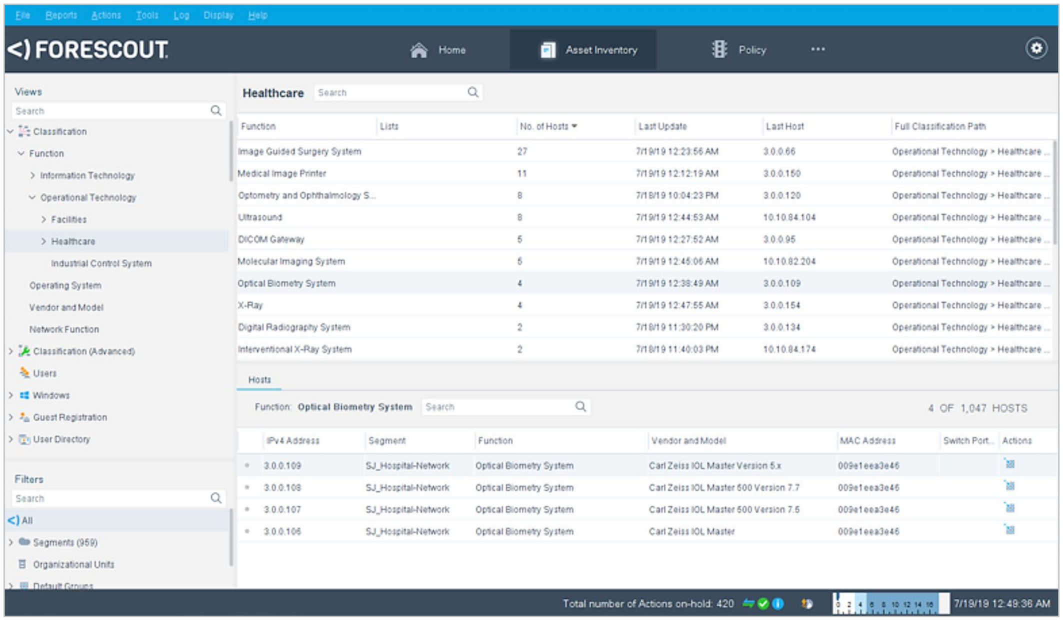
Organizations can use Forescout's asset inventory as a single source of insight into all of their assets. Or, they may continue to use their CMDB platform and create bidirectional communication between Forescout and the CMDB to send all of Forescout's device intelligence, including classification, in real time.

Network Extraction

Organizations can significantly increase asset discovery and asset intelligence by enabling network extraction through a SPAN/mirror port or a TAP. Forescout mines full packet capture data by performing protocol parsing and packet inspection and using the data to auto-classify devices into three dimensions: device function and type, OS and vendor and model.

Network monitoring is particularly important when it comes to ICS devices and OT networks. Forescout supports parsing more than 60 ICS protocols. When connected to a SPAN port at Supervisory, Level 3, of the Purdue model, the system uses the natural access control boundary and therefore allows for real-time OT device discovery through nonintrusive means.

Forescout has robust network extraction capabilities that also uniquely assist healthcare organizations. The platform has endpoint detection and classification support for the top 20 medical device manufacturers along with many others. Forescout can also handle medical imaging data flows and system traffic using the Digital Imaging and Communications in Medicine (DICOM) protocol. This protocol visibility is a huge boon for not just hospitals but all healthcare organizations, providing visibility for remote offices, diagnostic centers and any organization that consumes medical imaging, including insurance providers, medical colleges, and test and quality assurance environments. When Forescout is monitoring the network segments and DICOM data flows into monitored environments, organizations have a more complete picture of which devices are using imaging data. As a result, they have a more complete picture of protected health information, which helps ensure data security compliance. Figure 6 illustrates Forescout visibility into medical devices.



Healthcare

Function	Lists	No. of Hosts	Last Update	Last Host	Full Classification Path
Image Guided Surgery System		27	7/19/19 12:23:56 AM	3.0.0.66	Operational Technology > Healthcare ...
Medical Image Printer		11	7/19/19 12:12:19 AM	3.0.0.150	Operational Technology > Healthcare ...
Optometry and Ophthalmology S...		8	7/18/19 10:04:23 PM	3.0.0.120	Operational Technology > Healthcare ...
Ultrasound		8	7/19/19 12:44:53 AM	10.10.84.104	Operational Technology > Healthcare ...
DICOM Gateway		5	7/19/19 12:27:52 AM	3.0.0.95	Operational Technology > Healthcare ...
Molecular Imaging System		5	7/19/19 12:45:06 AM	10.10.82.204	Operational Technology > Healthcare ...
Optical Biometry System		4	7/19/19 12:38:49 AM	3.0.0.109	Operational Technology > Healthcare ...
X-Ray		4	7/19/19 12:47:55 AM	3.0.0.154	Operational Technology > Healthcare ...
Digital Radiography System		2	7/18/19 11:30:20 PM	3.0.0.134	Operational Technology > Healthcare ...
Interventional X-Ray System		2	7/18/19 11:40:03 PM	10.10.84.174	Operational Technology > Healthcare ...

Hosts

Function: **Optical Biometry System** 4 OF 1,047 HOSTS

IPv4 Address	Segment	Function	Vendor and Model	MAC Address	Switch Port...	Actions
3.0.0.109	SJ_Hospital-Network	Optical Biometry System	Carl Zeiss IOL Master Version 5.x	009e1eea3e46		
3.0.0.108	SJ_Hospital-Network	Optical Biometry System	Carl Zeiss IOL Master 500 Version 7.7	009e1eea3e46		
3.0.0.107	SJ_Hospital-Network	Optical Biometry System	Carl Zeiss IOL Master 500 Version 7.5	009e1eea3e46		
3.0.0.106	SJ_Hospital-Network	Optical Biometry System	Carl Zeiss IOL Master	009e1eea3e46		

Total number of Actions on-hold: 420 7/19/19 12:49:38 AM

Figure 6. Medical Device Classification by Device Function

Auto-classification

Accurately auto-classifying network assets based on observed data allows Forescout to create contextual policies based on device type. IoT and OT devices can't support an agent, which makes it necessary to look beyond traditional authentication approaches to apply access control policies.

The Forescout policy engine uses collected device intelligence to automate workflows for populating a CMDB. This will help keep the organization's CMDB current and accurate. Forescout can send an event to several different SIEM solutions via `syslog` or a more direct integration; apply network segmentation via integration with next-generation firewalls (NGFWs), network infrastructure and software-defined networking technologies; and notify an administrator of unknown devices.

Forescout's device auto-classification process has these main aspects:

- Agentless data collection (See examples provided in previous discussions of discovery and network extraction.)
- Ability to map device attributes to out-of-the-box device profiles, enabling devices to be classified by their function, OS and vendor and model
- Device sorting by OS and vendor and model, providing a full asset inventory
- Forescout device cloud, a crowdsourced device repository used to improve device identification (Organizations can still receive new device profiles if they choose to opt out of device cloud.)

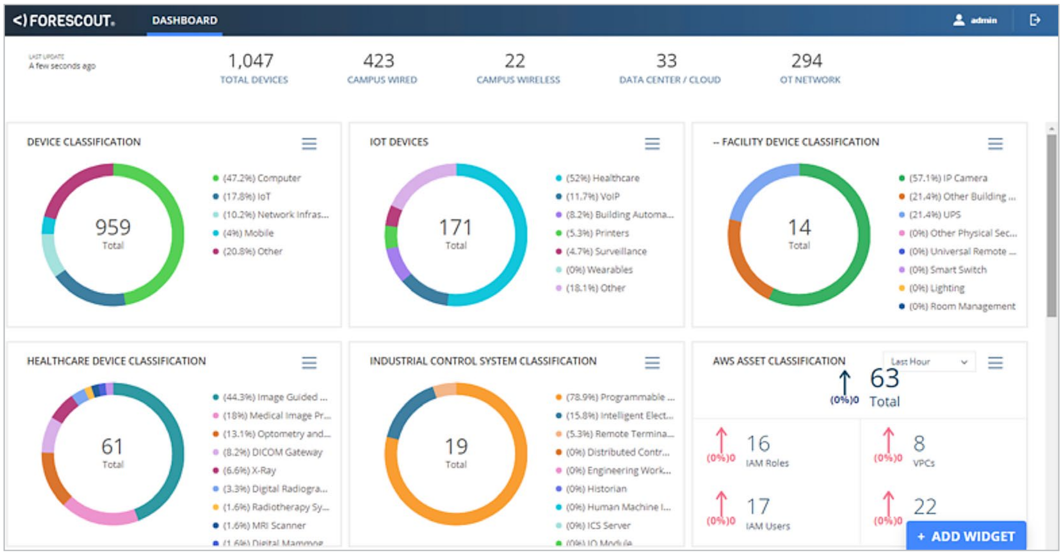


Figure 7. Results of Forescout's Automatic Device Classification

As illustrated in Figure 7, the Forescout classification engine maps devices into a wide variety of device profiles and functions.

Once device attributes are identified and classified, the endpoints are added to asset groups. When the engine cannot find an exact match, the analyst can manually classify the device and, if desired, share unknown device information with Forescout's device cloud R&D team. Forescout updates its device profile library on a monthly basis.

Risk Assessment and Device Compliance

Once analysts gain confidence and familiarity with Forescout 8.1's ability to discover and auto-classify devices, they can tap into the platform's risk assessment and device compliance capabilities. The platform has more than a dozen predefined policy enforcement templates that organizations can quickly adapt to meet their needs. For example, security teams can use Forescout's overall endpoint compliance template to assess client firewall status, remove unauthorized applications by application type and then check for specific compliance settings such as current antivirus and OS patch levels. Once the policy has been configured, system admins can roll the policy out by IP segment or apply a policy network-wide.

To provide a single source of truth for device compliance state, Forescout provides integrations with a variety of enterprise tools—including vulnerability assessment tools, endpoint protection tools, patch management, endpoint detection and response platforms, and IT service management systems.

The threat policy is also important to OT networks. As an example, organizations can configure this policy specifically to check for dual-homed systems, which can provide an unintended bridge between IT and OT networks.

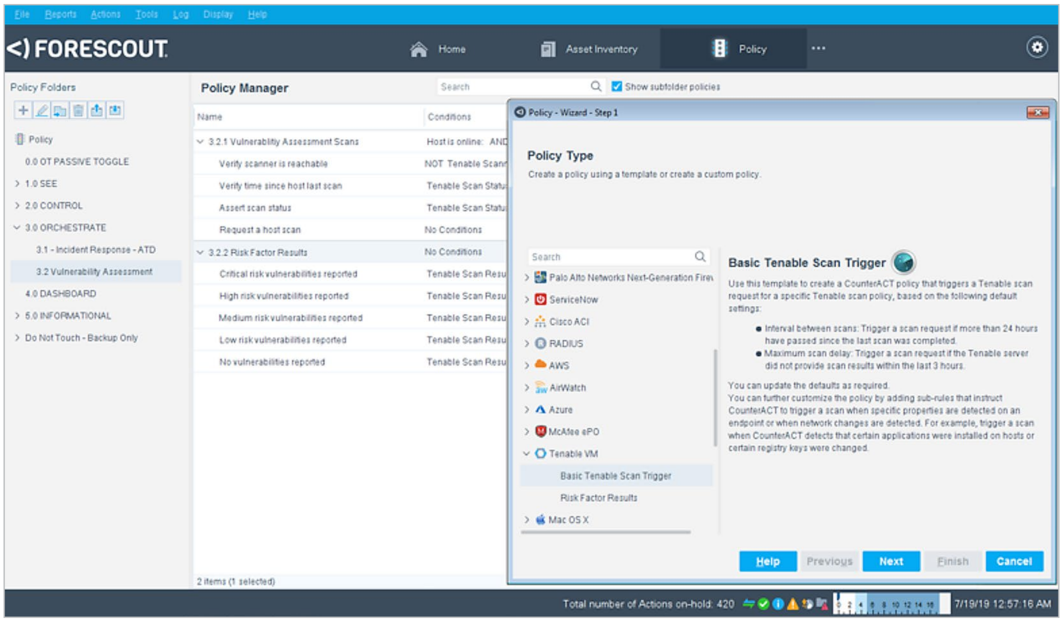
Maintaining Compliance

Not every device attached to the network is deployed in a secure configuration. This is why analysts can configure Forescout to assess risk in real time at a network admission event or soon after as a device is profiled, and then take appropriate action. In particular, organizations are adopting and installing IoT devices at an accelerated pace: HVAC, building monitoring, conference rooms, multifunction printers and the like can all benefit from Forescout's approach of assessing a device's posture as early as possible.

For enhanced risk posture assessment, Forescout integrates with mainstream vulnerability assessment (VA) scan tools. The Forescout platform enables organizations to initiate a VA scan for segments under network admission monitoring. Once the scan is complete, results can be sent back to Forescout. Analysts can remediate manually on a case-by-case basis, or the Forescout platform can be set to automate remediation. That means if the vulnerabilities are critical enough, the platform can isolate the endpoint onto a VLAN at the switch level or trigger installation of a patch by a patch management platform. These policies are provided out of the box (see Figure 8).

Forescout makes it easy to complete multiple compliance checks. Figure 9 illustrates a particular system within AWS being identified as out of compliance.

As shown in Figure 10, further detail detects how a system is out of compliance and highlights why that system failed its compliance check.



Name	Conditions
3.2.1 Vulnerablity Assessment Scans	Host is online: AND
Verify scanner is reachable	NOT Tenable Scan
Verify time since host last scan	Tenable Scan Statu
Assert scan status	Tenable Scan Statu
Request a host scan	No Conditions
3.2.2 Risk Factor Results	No Conditions
Critical risk vulnerabilities reported	Tenable Scan Resu
High risk vulnerabilities reported	Tenable Scan Resu
Medium risk vulnerabilities reported	Tenable Scan Resu
Low risk vulnerabilities reported	Tenable Scan Resu
No vulnerabilities reported	Tenable Scan Resu

2 items (1 selected)

Policy - Wizard - Step 1

Policy Type

Create a policy using a template or create a custom policy.

Search

- Palo Alto Networks Next-Generation Firev
- ServiceNow
- Cisco ACI
- RADIUS
- AWS
- AirWatch
- Azure
- McAfee ePO
- Tenable VM
  - Basic Tenable Scan Trigger
  - Risk Factor Results
- Mac OS X

Basic Tenable Scan Trigger

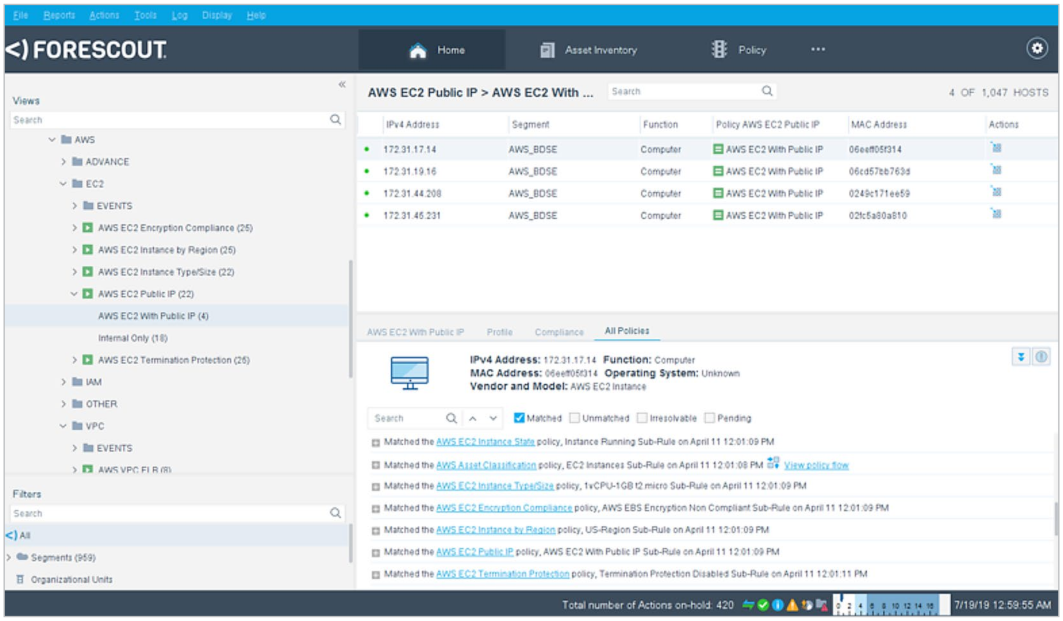
Use this template to create a CounterACT policy that triggers a Tenable scan request for a specific Tenable scan policy, based on the following default settings:

- Interval between scans: Trigger a scan request if more than 24 hours have passed since the last scan was completed.
- Maximum scan delay: Trigger a scan request if the Tenable server did not provide scan results within the last 3 hours.

You can update the defaults as required.
You can further customize the policy by adding sub-rules that instruct CounterACT to trigger a scan when specific properties are detected on an endpoint or when network changes are detected. For example, trigger a scan when CounterACT detects that certain applications were installed on hosts or certain registry keys were changed.

Total number of Actions on-hold: 420 7/19/19 12:57:16 AM

Figure 8. Adding a Vulnerability Assessment Policy to Scan Devices on Network Connection



AWS EC2 Public IP > AWS EC2 With ... 4 OF 1,047 HOSTS

IPv4 Address	Segment	Function	Policy AWS EC2 Public IP	MAC Address	Actions
172.31.17.14	AWS_BDSE	Computer	AWS EC2 With Public IP	06eeff05f314	
172.31.19.16	AWS_BDSE	Computer	AWS EC2 With Public IP	06cd57bb763d	
172.31.44.208	AWS_BDSE	Computer	AWS EC2 With Public IP	0249c171ee59	
172.31.45.231	AWS_BDSE	Computer	AWS EC2 With Public IP	02fc5a80a810	

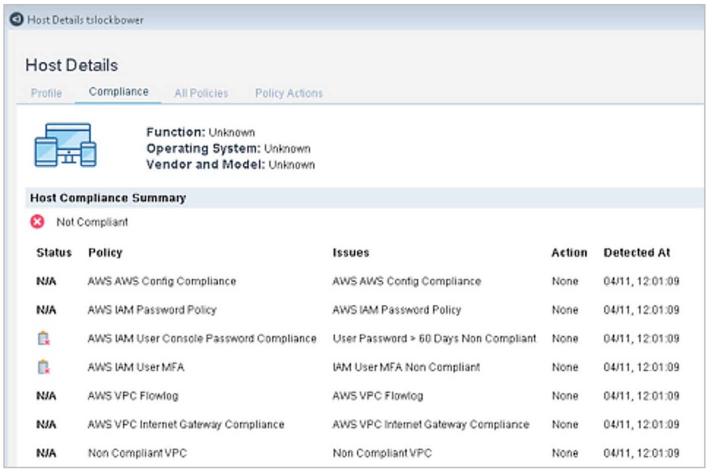
IPv4 Address: 172.31.17.14 **Function:** Computer
MAC Address: 06eeff05f314 **Operating System:** Unknown
Vendor and Model: AWS EC2 Instance

Search ☑ Matched □ Unmatched □ Irresolvable □ Pending

- Matched the AWS EC2 Instance State policy, Instance Running Sub-Rule on April 11 12:01:09 PM
- Matched the AWS Asset Classification policy, EC2 Instances Sub-Rule on April 11 12:01:08 PM View policy flow
- Matched the AWS EC2 Instance Type/Size policy, 1vCPU-1GB t2.micro Sub-Rule on April 11 12:01:09 PM
- Matched the AWS EC2 Encryption Compliance policy, AWS EBS Encryption Non Compliant Sub-Rule on April 11 12:01:09 PM
- Matched the AWS EC2 Instance by Region policy, US-Region Sub-Rule on April 11 12:01:09 PM
- Matched the AWS EC2 Public IP policy, AWS EC2 With Public IP Sub-Rule on April 11 12:01:09 PM
- Matched the AWS EC2 Termination Protection policy, Termination Protection Disabled Sub-Rule on April 11 12:01:11 PM

Total number of Actions on-hold: 420 7/19/19 12:59:55 AM

Figure 9. AWS System Compliance Failure



Host Details

Function: Unknown
Operating System: Unknown
Vendor and Model: Unknown

Host Compliance Summary

Not Compliant

Status	Policy	Issues	Action	Detected At
N/A	AWS AWS Config Compliance	AWS AWS Config Compliance	None	04/11, 12:01:09
N/A	AWS IAM Password Policy	AWS IAM Password Policy	None	04/11, 12:01:09
	AWS IAM User Console Password Compliance	User Password > 60 Days Non Compliant	None	04/11, 12:01:09
	AWS IAM User MFA	IAM User MFA Non Compliant	None	04/11, 12:01:09
N/A	AWS VPC Flowlog	AWS VPC Flowlog	None	04/11, 12:01:09
N/A	AWS VPC Internet Gateway Compliance	AWS VPC Internet Gateway Compliance	None	04/11, 12:01:09
N/A	Non Compliant VPC	Non Compliant VPC	None	04/11, 12:01:09

Figure 10. Forescout Noncompliance/Failure Detail

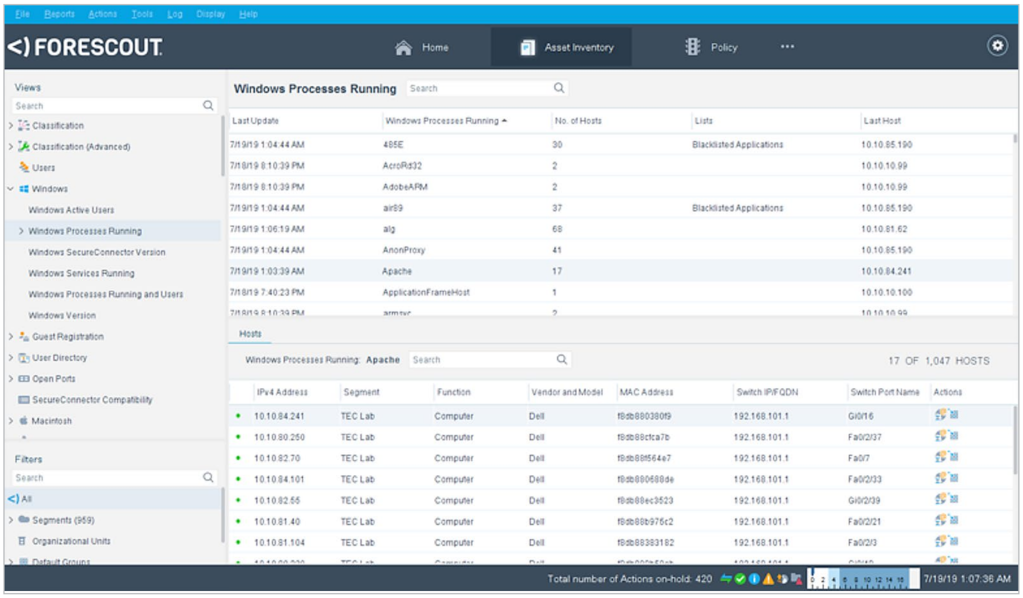
Because Forescout can perform WMI-based remote device query, it has application awareness and can apply that application awareness for several purposes. Figure 11 shows an alphabetical list of applications, how many hosts are running a given application or service and which applications are on the “Blacklisted applications” list.

These checks help the security team isolate malicious software or policy violations and help the operations team identify inappropriate applications in the environment. Quickly finding these results is another example of Forescout’s efficient interface, because with just a few clicks, the analyst has an inventory of suspect endpoints running processes that match a list of blacklisted software.

Forescout makes it very easy to identify where blacklisted applications are in the environment and which hosts were observed running those applications as of the last system check interval, as shown in Figure 12.

When possible, malware and adversaries will establish persistence on a system. They can do so in several ways, with Windows services being one of them. In this example, Forescout allows analysts to sort the service name inventory by hostname so that single or unique service names are easily visible. See Figure 13.

Some results might be easily explained (for example, in a network with one Windows Domain Controller, a single instance of the



Windows Processes Running

Last Update	Windows Processes Running ▲	No. of Hosts	Lists	Last Host
7/19/19 1:04:44 AM	485E	30	Blacklisted Applications	10.10.85.190
7/18/19 8:10:39 PM	AcroRd32	2		10.10.10.99
7/18/19 8:10:39 PM	AdobeARM	2		10.10.10.99
7/19/19 1:04:44 AM	air89	37	Blacklisted Applications	10.10.85.190
7/19/19 1:06:19 AM	alg	68		10.10.81.62
7/19/19 1:04:44 AM	AnonProxy	41		10.10.85.190
7/19/19 1:03:39 AM	Apache	17		10.10.84.241
7/18/19 7:40:23 PM	ApplicationFrameHost	1		10.10.10.100
7/18/19 8:10:39 PM	armsvc	2		10.10.10.99

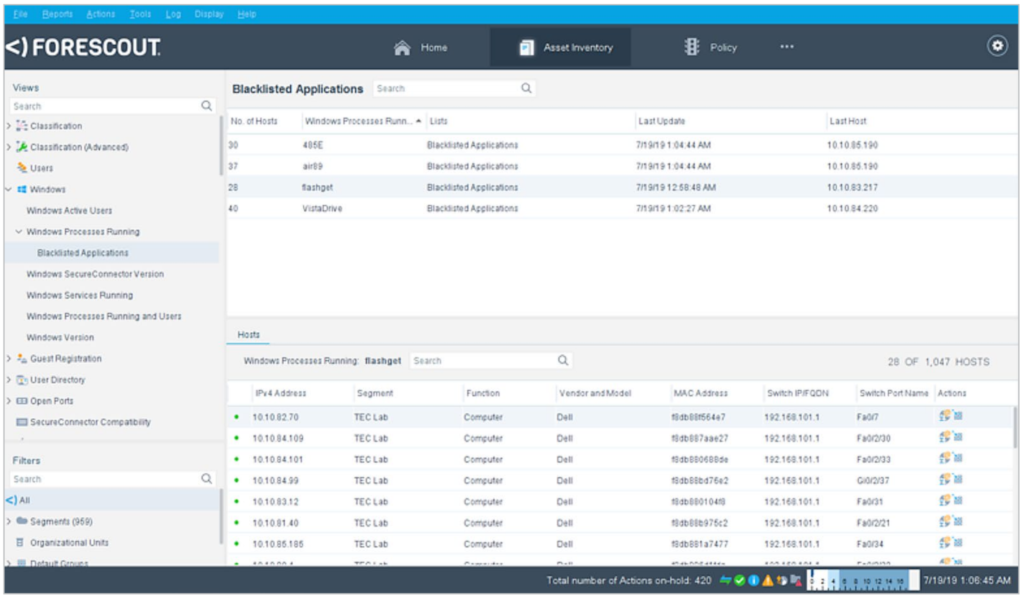
Hosts

Windows Processes Running: **Apache**   17 OF 1,047 HOSTS

	IPv4 Address	Segment	Function	Vendor and Model	MAC Address	Switch IP/FQDN	Switch Port Name	Actions
●	10.10.84.241	TEC Lab	Computer	Dell	f8db880380f9	192.168.101.1	Gi0/16	
●	10.10.80.250	TEC Lab	Computer	Dell	f8db88cfca7b	192.168.101.1	Fa0/2/37	
●	10.10.82.70	TEC Lab	Computer	Dell	f8db88f564e7	192.168.101.1	Fa0/7	
●	10.10.84.101	TEC Lab	Computer	Dell	f8db880688de	192.168.101.1	Fa0/2/33	
●	10.10.82.55	TEC Lab	Computer	Dell	f8db88ec3523	192.168.101.1	Gi0/2/39	
●	10.10.81.40	TEC Lab	Computer	Dell	f8db88b976c2	192.168.101.1	Fa0/2/21	
●	10.10.81.104	TEC Lab	Computer	Dell	f8db88383182	192.168.101.1	Fa0/2/3	

Total number of Actions on-hold: 420   7/19/19 1:07:36 AM

Figure 11. Process Identification, Including Blacklisted Applications



Blacklisted Applications

No. of Hosts	Windows Processes Runn... ▲	Lists	Last Update	Last Host
30	485E	Blacklisted Applications	7/19/19 1:04:44 AM	10.10.85.190
37	air89	Blacklisted Applications	7/19/19 1:04:44 AM	10.10.85.190
28	flashget	Blacklisted Applications	7/19/19 12:58:48 AM	10.10.83.217
40	VistaDrive	Blacklisted Applications	7/19/19 1:02:27 AM	10.10.84.220

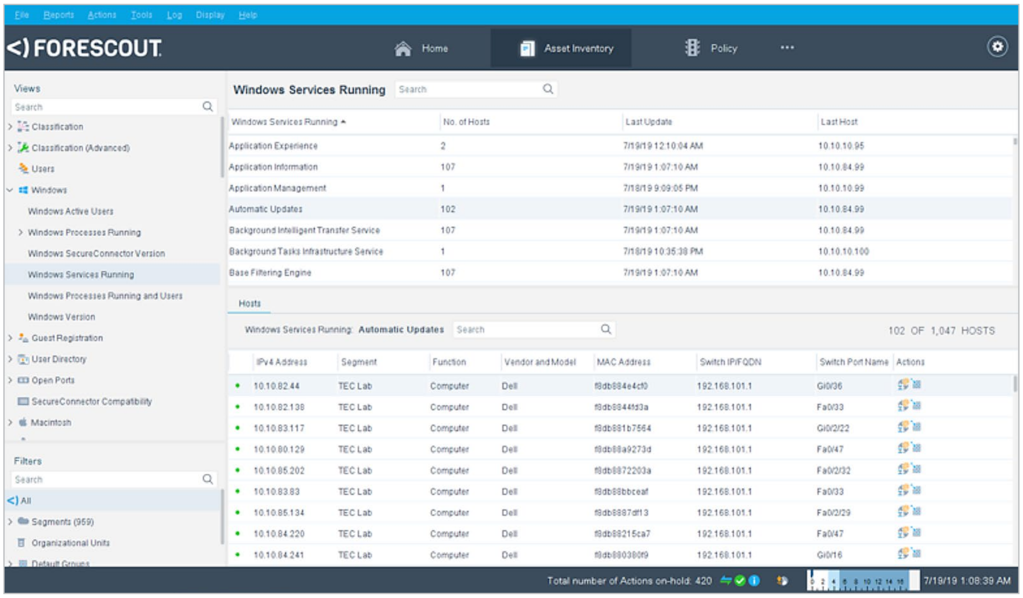
Hosts

Windows Processes Running: **flashget**   28 OF 1,047 HOSTS

	IPv4 Address	Segment	Function	Vendor and Model	MAC Address	Switch IP/FQDN	Switch Port Name	Actions
●	10.10.82.70	TEC Lab	Computer	Dell	f8db88f564e7	192.168.101.1	Fa0/7	
●	10.10.84.109	TEC Lab	Computer	Dell	f8db887aae27	192.168.101.1	Fa0/2/30	
●	10.10.84.101	TEC Lab	Computer	Dell	f8db880688de	192.168.101.1	Fa0/2/33	
●	10.10.84.99	TEC Lab	Computer	Dell	f8db88bd76e2	192.168.101.1	Gi0/2/37	
●	10.10.83.12	TEC Lab	Computer	Dell	f8db880104f8	192.168.101.1	Fa0/31	
●	10.10.81.40	TEC Lab	Computer	Dell	f8db88b976c2	192.168.101.1	Fa0/2/21	
●	10.10.85.186	TEC Lab	Computer	Dell	f8db881a7477	192.168.101.1	Fa0/34	

Total number of Actions on-hold: 420   7/19/19 1:06:45 AM

Figure 12. Processes Identified by Blacklist Policy



Windows Services Running

Windows Services Running ▲	No. of Hosts	Last Update	Last Host
Application Experience	2	7/19/19 12:10:04 AM	10.10.10.95
Application Information	107	7/19/19 1:07:10 AM	10.10.84.99
Application Management	1	7/18/19 9:09:05 PM	10.10.10.99
Automatic Updates	102	7/19/19 1:07:10 AM	10.10.84.99
Background Intelligent Transfer Service	107	7/19/19 1:07:10 AM	10.10.84.99
Background Tasks Infrastructure Service	1	7/18/19 10:35:38 PM	10.10.10.100
Base Filtering Engine	107	7/19/19 1:07:10 AM	10.10.84.99

Hosts

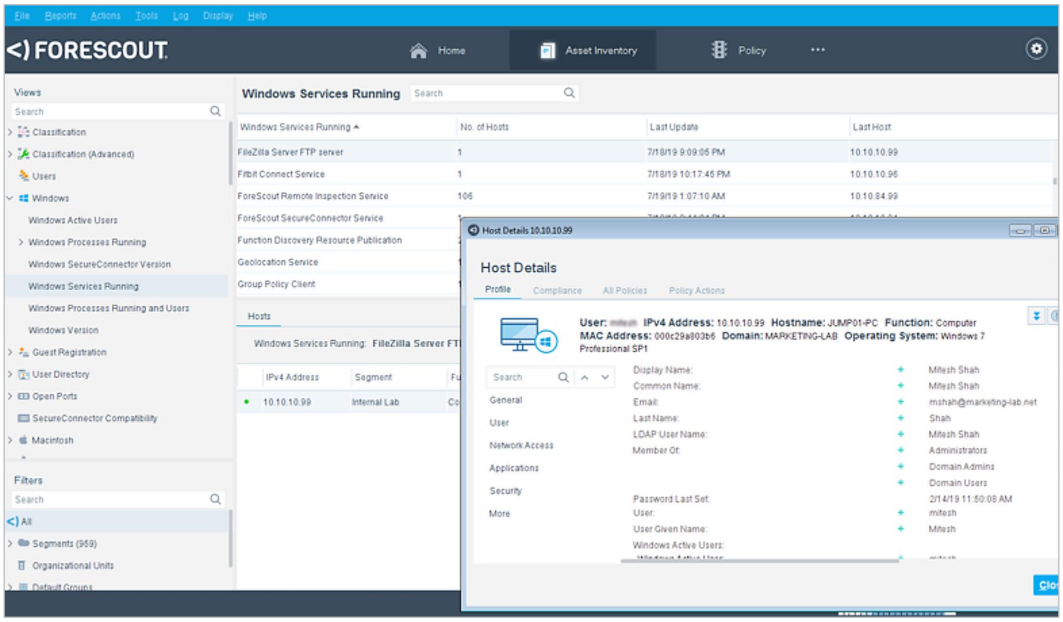
Windows Services Running: **Automatic Updates**   102 OF 1,047 HOSTS

	IPv4 Address	Segment	Function	Vendor and Model	MAC Address	Switch IP/FQDN	Switch Port Name	Actions
●	10.10.82.44	TEC Lab	Computer	Dell	f8db884e4cf0	192.168.101.1	Gi0/36	
●	10.10.82.138	TEC Lab	Computer	Dell	f8db8844fd3a	192.168.101.1	Fa0/33	
●	10.10.83.117	TEC Lab	Computer	Dell	f8db881b7564	192.168.101.1	Gi0/2/22	
●	10.10.80.129	TEC Lab	Computer	Dell	f8db88a9273d	192.168.101.1	Fa0/47	
●	10.10.85.202	TEC Lab	Computer	Dell	f8db8872203a	192.168.101.1	Fa0/2/32	
●	10.10.83.83	TEC Lab	Computer	Dell	f8db88bbceaf	192.168.101.1	Fa0/33	
●	10.10.85.134	TEC Lab	Computer	Dell	f8db8887df13	192.168.101.1	Fa0/2/29	
●	10.10.84.220	TEC Lab	Computer	Dell	f8db88215ca7	192.168.101.1	Fa0/47	
●	10.10.84.241	TEC Lab	Computer	Dell	f8db880380f9	192.168.101.1	Gi0/16	

Total number of Actions on-hold: 420   7/19/19 1:08:39 AM

Figure 13. Alphabetical List of Services in the Environment

DNS service makes sense), but a "FileZilla" service, as seen in Figure 14, may not be authorized. Forescout makes it very easy to identify the system involved and will show the last known user in the asset details. Figure 14 also shows that the user details pane includes key user attributes, saving the analyst from having to consult a secondary system to retrieve critical properties, including group membership, email address and account status.



Windows Services Running

Windows Services Running ▲	No. of Hosts	Last Update	Last Host
FileZilla Server FTP server	1	7/18/19 9:09:05 PM	10.10.10.99
Fitbit Connect Service	1	7/18/19 10:17:45 PM	10.10.10.96
ForeScout Remote Inspection Service	106	7/19/19 1:07:10 AM	10.10.84.99
ForeScout SecureConnector Service			
Function Discovery Resource Publication			
Geolocation Service			
Group Policy Client			

Windows Services Running: **FileZilla Server FT**

	IPv4 Address	Segment	Fu
●	10.10.10.99	Internal Lab	Co

Host Details

User: [redacted] **IPv4 Address:** 10.10.10.99 **Hostname:** JUMP01-PC **Function:** Computer
MAC Address: 000c29a803b6 **Domain:** MARKETING-LAB **Operating System:** Windows 7 Professional SP1

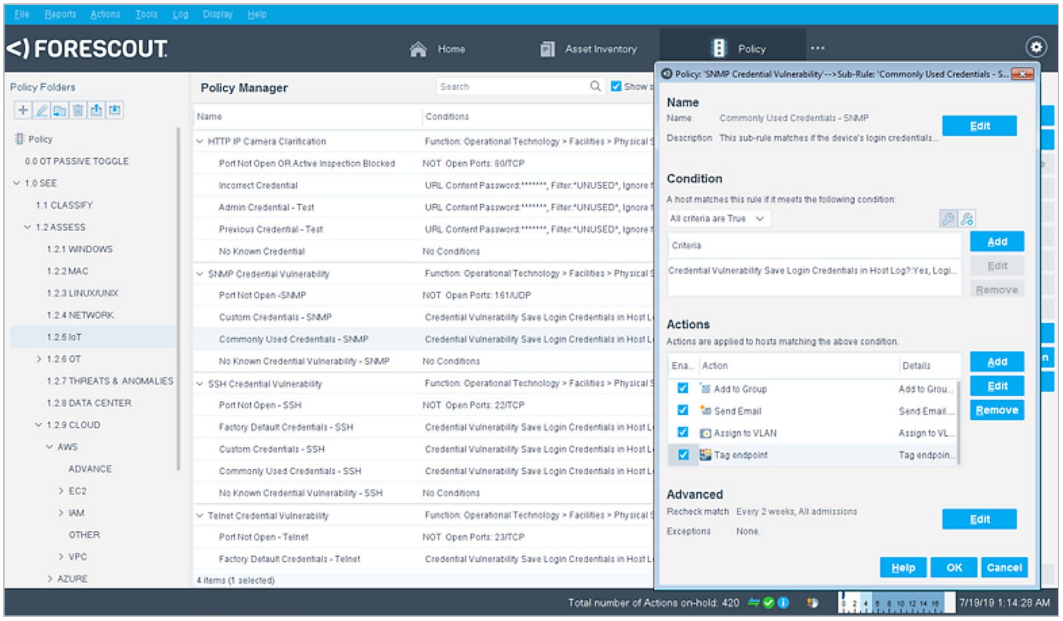
Display Name:	+	Mitesh Shah
Common Name:	+	Mitesh Shah
Email:	+	mshah@marketing-lab.net
Last Name:	+	Shah
LDAP User Name:	+	Mitesh Shah
Member Of:	+	Administrators
	+	Domain Admins
	+	Domain Users
Password Last Set:		2/14/19 11:50:08 AM
User:	+	mitesh
User Given Name:	+	Mitesh
Windows Active Users:		

Figure 14. Potentially Suspect Windows Service

This figure shows yet another stellar example of Forescout's highly efficient interface, data collection and data presentation. By making key details of the investigation accessible in a single user interface view, Forescout has minimized the hours analysts need to invest in this process.

IoT Device Proliferation and Assessment

Organizations today are adding devices that support all kinds of automation—running the gamut from IP cameras and network display devices to HVAC controllers, environmental monitoring stations, and security and fire control systems. It seems that every semi-intelligent device has an RJ-45 jack or built-in wireless. Because of this near ubiquity, device proliferation is a very real problem. The Forescout platform can help minimize risk presented by IoT device proliferation. First, the platform can discover and classify all IoT devices so there are no blind spots. Next, it can detect factory default or weak, commonly used credentials on network endpoints by leveraging its built-in credential database for SSH, Telnet and SNMP protocols. Overall, Forescout can mitigate risk through device discovery and classification as well as by assessing IoT devices, alerting analysts and proactively limiting or blocking the device from the network, as illustrated in Figure 15.



Policy Manager

Name	Conditions
HTTP IP Camera Clarification	Function: Operational Technology > Facilities > Physical S
Port Not Open OR Active Inspection Blocked	NOT Open Ports: 80/TCP
Incorrect Credential	URL Content Password:*******, Filter:"UNUSED", Ignore f
Admin Credential - Test	URL Content Password:*******, Filter:"UNUSED", Ignore f
Previous Credential - Test	URL Content Password:*******, Filter:"UNUSED", Ignore f
No Known Credential	No Conditions
SNMP Credential Vulnerability	Function: Operational Technology > Facilities > Physical S
Port Not Open -SNMP	NOT Open Ports: 161/UDP
Custom Credentials - SNMP	Credential Vulnerability Save Login Credentials in Host L
Commonly Used Credentials - SNMP	Credential Vulnerability Save Login Credentials in Host L
No Known Credential Vulnerability - SNMP	No Conditions
SSH Credential Vulnerability	Function: Operational Technology > Facilities > Physical S
Port Not Open - SSH	NOT Open Ports: 22/TCP
Factory Default Credentials - SSH	Credential Vulnerability Save Login Credentials in Host L
Custom Credentials - SSH	Credential Vulnerability Save Login Credentials in Host L
Commonly Used Credentials - SSH	Credential Vulnerability Save Login Credentials in Host L
No Known Credential Vulnerability - SSH	No Conditions
Telnet Credential Vulnerability	Function: Operational Technology > Facilities > Physical S
Port Not Open - Telnet	NOT Open Ports: 23/TCP
Factory Default Credentials - Telnet	Credential Vulnerability Save Login Credentials in Host L

4 items (1 selected)

Policy: 'SNMP Credential Vulnerability'-->Sub-Rule: 'Commonly Used Credentials - S...

Name
Name: Commonly Used Credentials - SNMP
Description: This sub-rule matches if the device's login credentials...

Condition
A host matches this rule if it meets the following condition:
All criteria are True

Criteria
Credential Vulnerability Save Login Credentials in Host Log?:Yes, Logi...

Actions
Actions are applied to hosts matching the above condition.

Ena...	Action	Details
☑	Add to Group	Add to Grou...
☑	Send Email	Send Email...
☑	Assign to VLAN	Assign to VL...
☑	Tag endpoint	Tag endpoin...

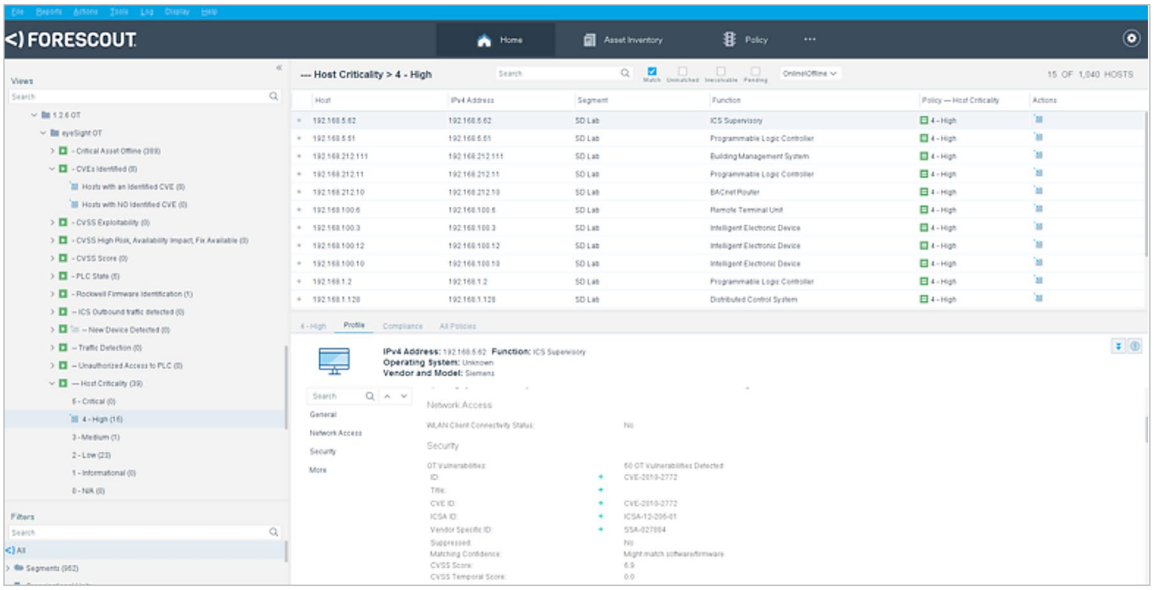
Advanced
Recheck match: Every 2 weeks, All admissions
Exceptions: None.

Total number of Actions on-hold: 420 7/19/19 1:14:28 AM

Figure 15. Device Classification Policy for IoT

OT Vulnerability Assessment

New as of version 8.1, Forescout can passively scan OT/ICS devices for vulnerabilities to ensure that OT/ICS processes are not adversely affected. Figure 16 is an example that shows devices Forescout found with a “High” host criticality level.


File Reports Actions Tools Log Display Help
<) FORESCOUT
Home
Asset Inventory
Policy
Views
Search
1.2.6 OT
eyeSight OT
- Critical Asset Offline (389)
- CVEs Identified (0)
Hosts with an Identified CVE (0)
Hosts with NO Identified CVE (0)
- CVSS Exploitability (0)
- CVSS High Risk, Availability Impact, Fix Available (0)
- CVSS Score (0)
- PLC State (6)
- Rockwell Firmware Identification (1)
-- ICS Outbound traffic detected (0)
-- New Device Detected (0)
-- Traffic Detection (0)
-- Unauthorized Access to PLC (0)
--- Host Criticality (39)
5 - Critical (0)
4 - High (16)
3 - Medium (1)
2 - Low (23)
1 - Informational (0)
0 - N/A (0)
Filters
Search
All
Segments (962)
--- Host Criticality > 4 - High
Search
Match
Unmatched
Irresolvable
Pending
Online/Offline
15 OF 1,040 HOSTS

Host	IPv4 Address	Segment	Function	Policy — Host Criticality	Actions
192.168.5.62	192.168.5.62	SD Lab	ICS Supervisory	4 - High	
192.168.5.61	192.168.5.61	SD Lab	Programmable Logic Controller	4 - High	
192.168.212.111	192.168.212.111	SD Lab	Building Management System	4 - High	
192.168.212.11	192.168.212.11	SD Lab	Programmable Logic Controller	4 - High	
192.168.212.10	192.168.212.10	SD Lab	BACnet Router	4 - High	
192.168.100.6	192.168.100.6	SD Lab	Remote Terminal Unit	4 - High	
192.168.100.3	192.168.100.3	SD Lab	Intelligent Electronic Device	4 - High	
192.168.100.12	192.168.100.12	SD Lab	Intelligent Electronic Device	4 - High	
192.168.100.10	192.168.100.10	SD Lab	Intelligent Electronic Device	4 - High	
192.168.1.2	192.168.1.2	SD Lab	Programmable Logic Controller	4 - High	
192.168.1.128	192.168.1.128	SD Lab	Distributed Control System	4 - High	

IPv4 Address: 192.168.5.62 **Function:** ICS Supervisory
Operating System: Unknown
Vendor and Model: Siemens

Network Access

WLAN Client Connectivity Status: Nil

Security

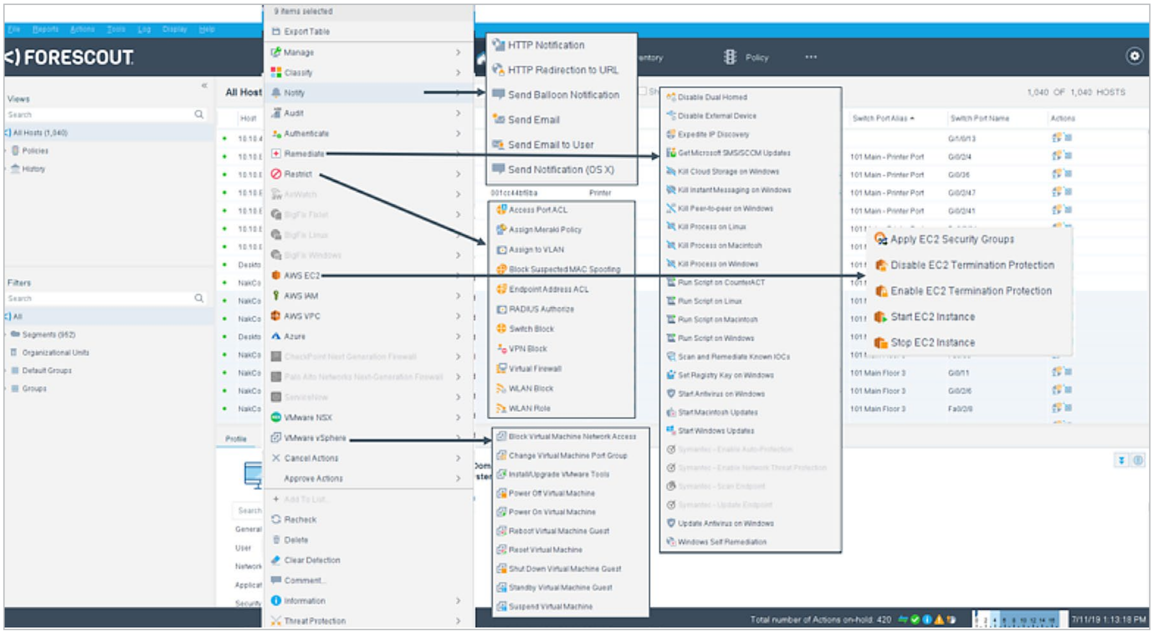
OT Vulnerabilities: 60 OT Vulnerabilities Detected
ID: CVE-2010-2772
Title:
CVE ID: CVE-2010-2772
ICSA ID: ICSA-12-205-01
Vendor Specific ID: SSA-027884
Suppressed: Nil
Matching Confidence: Might match software/firmware
CVSS Score: 6.9
CVSS Temporal Score: 0.0

Figure 16. Assessing OT Device Risk

Automating Controls

So far, several examples presented demonstrate Forescout’s ability to automate host and network controls. For example, the platform inspects devices continuously and can take a specific host or network action if a device’s compliance state changes. Examples include launching a network scan or vulnerability scan, forcing antivirus or patch updates or taking an action on systems with blacklisted applications. The platform can also send user notifications via email, browser or balloon pop-up prior to enforcing any host or network controls, so users have the chance to self-remediate. The platform can also restrict devices to specific segments via VLANs, access control lists (ACLs), virtual firewalls and NGFW tags; perform IoT device and credential checks; and launch a variety of cyber incident response scenarios.

Figure 17 shows some of the control actions Forescout provides as configured by default. All of these actions can be automated using Forescout’s robust policy engine framework, which uses simple if/else Boolean logic, making the platform easy to use and configure.



Switch Port Alias	Switch Port Name	Actions
	Gi1/0/13	
101 Main - Printer Port	Gi0/2/4	
101 Main - Printer Port	Gi0/36	
101 Main - Printer Port	Gi0/2/47	
101 Main - Printer Port	Gi0/2/41	
101 Main Floor 3	Gi0/11	
101 Main Floor 3	Gi0/2/6	
101 Main Floor 3	Fa0/2/8	

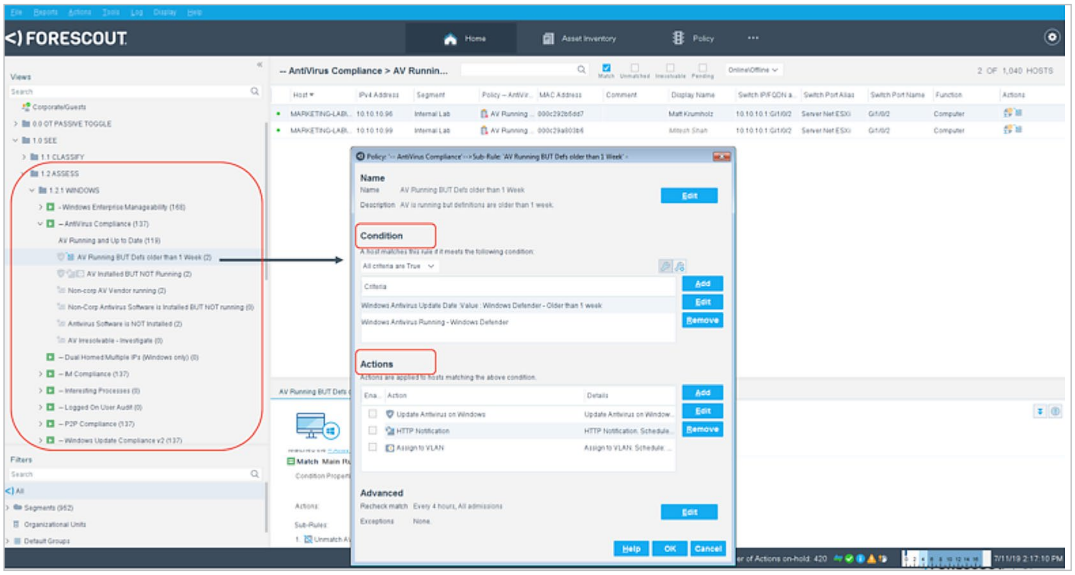
Figure 17. Forescout’s Host and Network Control Actions

Device Auto-mapping into Target VLAN

As previously discussed, Forescout classifies and assesses devices on initial network connection and continuously for as long as they are on the corporate network. As the system identifies users or devices in particular groups—for example, human resources, IT, finance, call center, printers and IP cameras—the system can segregate these users into their respective VLANs or apply a restrictive ACL (be it custom developed or chosen from an ACL library) on the switch. These functions provide 802.1X-like behavior without the deployment complexity or requirements for network redesign or any hardware and software upgrades.

Device Auto-remediation

Forescout's policy engine makes it easy to view and edit a policy definition as appropriate. For example, corporate endpoints require that antivirus be installed and running. Sometimes these agents get out of date or a user with elevated access has either stopped or disabled the service. Upon connecting to the network, Forescout can detect that the antivirus agent is installed and enabled. If definitions are older than one week, it can remediate the devices by updating the antivirus on the endpoints and then notify users that the antivirus is being updated on their system. Organizations can opt to also apply network restrictions while the device is being remediated; as shown in Figure 18, we could limit network access until remediation is complete by putting this device into a restricted VLAN.


File Reports Actions Tools Log Display Help
<) FORESCOUT
Home
Asset Inventory
Policy
···
Views
Search
Corporate/Guests
0.0 OT PASSIVE TOGGLE
1.0 SEE
1.1 CLASSIFY
1.2 ASSESS
1.2.1 WINDOWS
- Windows Enterprise Manageability (168)
– AntiVirus Compliance (137)
AV Running and Up to Date (119)
AV Running BUT Defs older than 1 Week (2)
AV Installed BUT NOT Running (2)
Non-corp AV Vendor running (2)
Non-Corp Antivirus Software is Installed BUT NOT running (0)
Antivirus Software is NOT Installed (2)
AV Irresolvable - Investigate (0)
– Dual Homed/Multiple IPs (Windows only) (0)
– IM Compliance (137)
– Interesting Processes (0)
– Logged On User Audit (0)
– P2P Compliance (137)
– Windows Update Compliance v2 (137)
Filters
Search
<) All
Segments (952)
Organizational Units
Default Groups
-- AntiVirus Compliance > AV Runnin...
☑ Match □ Unmatched □ Irresolvable □ Pending
Online\Offline
2 OF 1,040 HOSTS

Host ▾	IPv4 Address	Segment	Policy – AntiVir...	MAC Address	Comment	Display Name	Switch IP/FQDN a...	Switch Port Alias	Switch Port Name	Function	Actions
MARKETING-LAB...	10.10.10.96	Internal Lab	AV Running ...	000c292b6dd7		Matt Krumholz	10.10.10.1:Gi1/0/2	Server Net ESXi	Gi1/0/2	Computer	
MARKETING-LAB...	10.10.10.99	Internal Lab	AV Running ...	000c29a803b6		Mitesh Shah	10.10.10.1:Gi1/0/2	Server Net ESXi	Gi1/0/2	Computer	

Policy: '-- AntiVirus Compliance'-->Sub-Rule: 'AV Running BUT Defs older than 1 Week' -

Name

Name: AV Running BUT Defs older than 1 Week

Description: AV is running but definitions are older than 1 week.

Condition

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

All criteria are True

Criteria:
- Windows Antivirus Update Date: Value : Windows Defender - Older than 1 week
- Windows Antivirus Running - Windows Defender

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
□	Update Antivirus on Windows	Update Antivirus on Window...
□	HTTP Notification	HTTP Notification: Schedule...
□	Assign to VLAN	Assign to VLAN: Schedule: ...

Advanced

Recheck match: Every 4 hours, All admissions

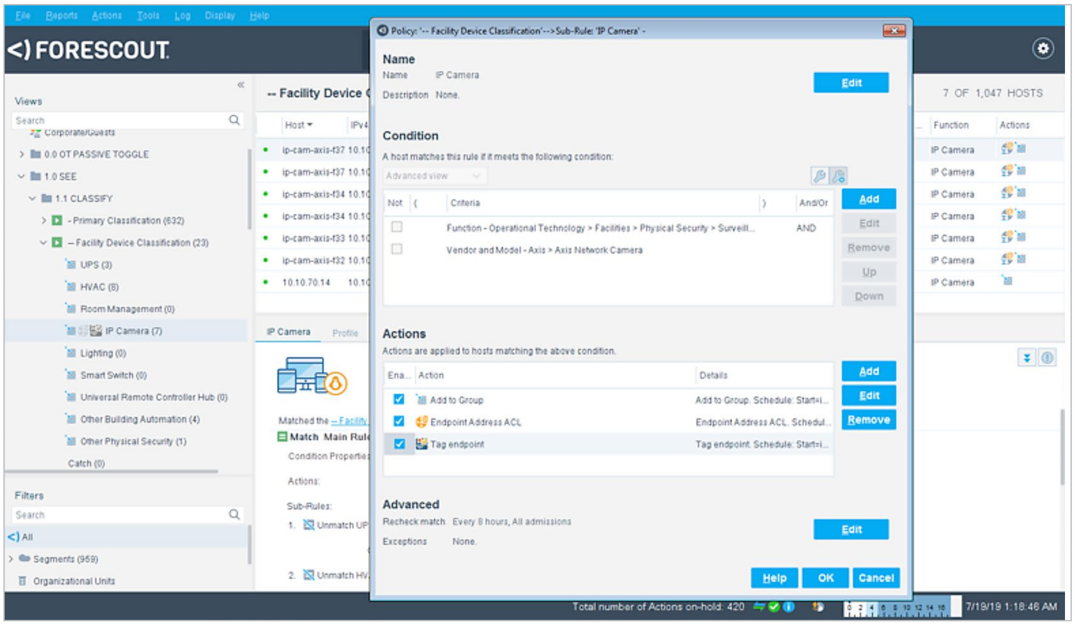
Exceptions: None.

Figure 18. Restrict Network Access for Device

IoT Device Segmentation

With more and more devices that can't support an agent or authentication when connecting to the network, it's important to apply a strategy to onboard these devices securely. For example, a marketing user doesn't need to have access to IP cameras. Forescout's classification and control automation allows analysts to segment IoT devices into their own zone, thereby ensuring only credentialed users can access IP cameras and that the IP cameras talk to only DVR recorders. Because Forescout integrates with leading switch and NGFW vendors, it provides flexibility to enforce segmentation at multiple network layers based on the network design. For example, segmentation can be enforced at the switch layer by ACLs or VLANs, or it can also be enforced by the NGFW if some of your access switches don't support ACLs.

Figure 19 shows an example of an IP camera being placed in its own segment via ACL and NGFW tags, with access limited to privileged admin users and DVR recorders.



Policy: '-- Facility Device Classification'-->Sub-Rule: 'IP Camera' -

Name

Name: IP Camera

Description: None.

Condition

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

Not	(	Criteria	)	And/Or
□		Function - Operational Technology > Facilities > Physical Security > Surveill...		AND
□		Vendor and Model - Axis > Axis Network Camera		

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
☑	Add to Group	Add to Group. Schedule: Start=i...
☑	Endpoint Address ACL	Endpoint Address ACL. Schedul...
☑	Tag endpoint	Tag endpoint. Schedule: Start=i...

Advanced

Recheck match: Every 8 hours, All admissions

Exceptions: None.

Total number of Actions on-hold: 420

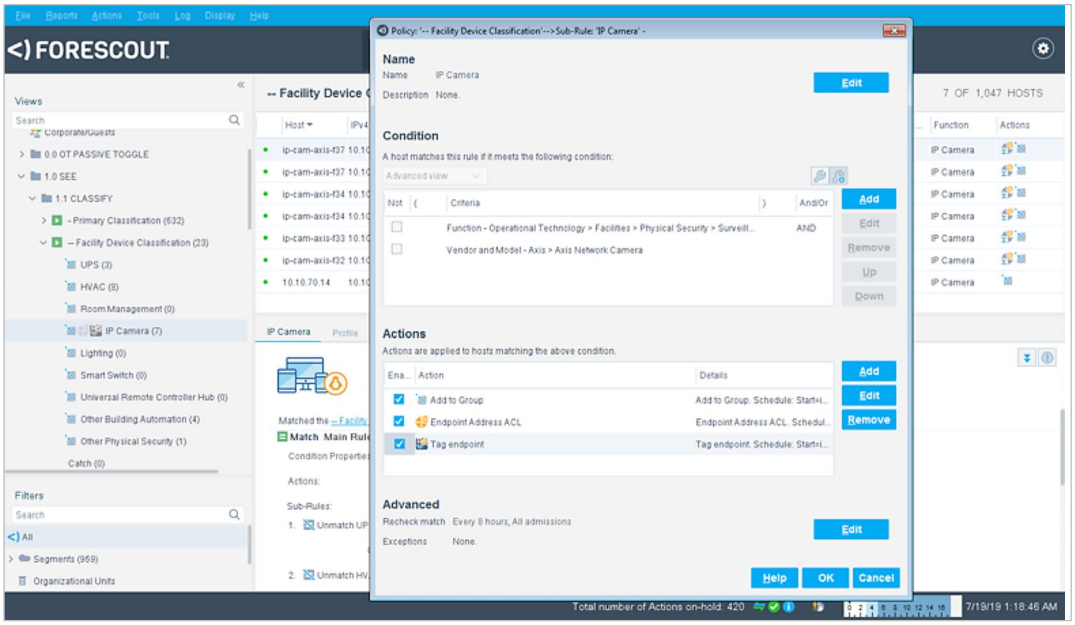
Figure 19. Automating IP Camera Segmentation

Incident Response for Known IoCs and Threat Intelligence

One of the core SANS tenets is, "Prevention is ideal; detection is a must; and detection without response is useless." Forescout's indicators of compromise (IoC) integration and scanning modules enable an enterprise to adhere to this philosophy: The platform's threat hunting capabilities enable security teams to keep up with recent threats. Forescout has a wide variety of capabilities in the IoC integration module, which can be fed by a variety of threat intelligence providers. We identified five of the most useful capabilities and the scenarios they help resolve by automating host and network controls:

- **Known file IoCs stored as both a binary file hash identifier and a process identifier—**Because of this, Forescout can kill off a suspect binary that's found running, while files present on disk can trigger further action.
- **Real-time monitoring—**Forescout's automation capabilities allow it to monitor real-time network sessions for command-and-control (C2) IP addresses and DNS hostname queries. If a device is communicating to a C2 IP address or DNS name, it can be found, whether it is managed or not. The platform can automatically restrict or block access from vulnerable devices and send a notification to the administrator.
- **System scans for potential abnormalities—**Upon initial connection to the network for a NAC-monitored segment, the platform scans the endpoint for known hash values and registry key entries, the presence of a file identified by a hash value, an installed service by name and mutex objects. Forescout handles scanning for these points because malware can use any of these techniques as it executes on a system. The resulting IoC table can be exported, so security admins can build up a history of IoC criteria used over time.
- **Notifications—**Like other policies defined within the system, Forescout can notify an admin via email or initiate a remediation action, reducing the time required before action can be taken on a potential threat.

- **IoC repository—**Forescout's IoC repository stores key details: date reported, severity, threat intel source, and name and file details (name, hash and type, and size). For example, if a host protection system notifies a security analyst that it has identified a new malicious browser extension, the analyst can add this IoC to the inventory as a "user-defined" IoC, sweep the enterprise and remediate as necessary (see Figure 20).



Policy: '-- Facility Device Classification'-->Sub-Rule: 'IP Camera' -

Name

Name IP Camera

Description None.

Condition

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

Not	(	Criteria	)	And/Or
□		Function - Operational Technology > Facilities > Physical Security > Surveill...		AND
□		Vendor and Model - Axis > Axis Network Camera		

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
☑	Add to Group	Add to Group. Schedule: Start=i...
☑	Endpoint Address ACL	Endpoint Address ACL. Schedul...
☑	Tag endpoint	Tag endpoint. Schedule: Start=i...

Advanced

Recheck match Every 8 hours, All admissions

Exceptions None.

Figure 20. A Forescout Site-Specific Hash Check for Suspect Binary

Orchestration Through Integration

Forescout provides a wide variety of direct integrations with third-party systems that help maximize your IT investment. With the right integration, the intelligence and capability of one system can be applied across the enterprise so the contextual insight provided by a focused, targeted solution can be generally applied elsewhere. Let's look at one of the many use cases Forescout can solve through integration.

For example, Forescout has integrations with several endpoint detection and response (EDR) solutions. EDR applications are more likely to be licensed and provisioned for end-user systems because the end user is a common target for attackers. We identified two common EDR scenarios in which Forescout can be useful:

- **EDR agent to IP segment validation—**Forescout can run a check against IP segments that should have an EDR agent as the endpoint connects to the network and is within scope for a given EDR deployment. For example, a user may connect a laptop or computer to the network that was moved from one location to another. If the agent is not present, Forescout can notify an administrator, push the client to a remediation network, initiate EDR agent installation and even restrict access to the network.
- **Attack alerts and IT hygiene—**When an EDR platform detects an issue, it can share an indicator of attack (IoA) or IoC with Forescout, including details such as the file hash. Forescout can restrict or block access from that malicious device and take that IoA/IoC and search the network for similar matches.

Enterprise Scalability and Flexibility

Like many mature enterprise management systems, the Forescout platform can be deployed across devices using different models—centralized, decentralized or hybrid—and can include a mix of physical and virtual appliances. The platform supports failover clustering for organizations with a need for high resiliency.

A centralized deployment will co-locate all appliances in a primary data center and then configure a variety of forwarding techniques for remote locations. A decentralized deployment has appliances sized for network segments based on the number of endpoints and LAN monitoring requirements, with distributed devices reporting back to a central enterprise manager. Hybrid models mix these centralized and decentralized models; for larger sites, a dedicated appliance can be deployed, while for smaller remote locations Forescout can use other passive collection techniques (DHCP helper, NetFlow, infrastructure polling, etc.) to achieve device visibility without deploying appliances at every site. Organizations can deploy different-sized appliances at different locations. Larger devices have a higher port density, which supports multiple SPAN ports for network extraction functionality.

Conclusion

The Forescout platform is a strong addition to the infrastructure stack for the enterprise because it provides holistic device visibility and control from the first point a device touches the network or is provisioned in either VMware, AWS or Azure. Once devices are identified, its full-stack management capabilities provide the foundational elements to keep devices off the corporate network that don't belong, maintain the devices that should be on the corporate network and provide an orchestration platform for IT, IoT and OT devices.

Forescout is much more than a device data collection and presentation platform. The platform can leverage the breadth of collected data to provide holistic device visibility, use all of that data to take action against misconfigured endpoints and maintain the organization's security posture. It can also integrate with many other related products and pull data from secondary systems. Collectively, these capabilities can further strengthen the overall organizational security state.

About the Author

Don Murdoch is a SANS community instructor specializing in incident response and security operations. A solutions-oriented IT director and consultant, he has hands-on experience leading software/infrastructure/system development efforts for financial and healthcare systems, including requirements definition, executive-level strategy and communications, solution design, architecture, deployment, production and dissolution. Don is the author of two prominent blue team handbooks, the first of which focuses on incident response and the second on SOC, SIEM and threat hunting. He holds the SANS GSE, Cyber Guardian Red and Blue Team and 17 other GIAC certifications, and he is also a certified TOGAF Enterprise Architect and SABSA Chartered Security Architect. Don is the author of two industry-impacting Blue Team Handbooks.

Sponsor

SANS would like to thank this paper's sponsor:

FORESCOUT®