CSO FROM IDG

August 16, 2018 www.csoonline.com

REVIEW

Review: Monitoring IT, OT and IoT devices with ForeScout

ForeScout is one of a very few programs that can help to track and manage operational technology and IoT devices alongside of information technology. Everything from lighting controllers to HVAC units can be discovered and managed.

By John Breeden II

Looked at very simplistically, most cybersecurity programs are simply trying to keep malicious programs from negatively affecting network assets. But to accomplish that, it helps to know exactly what those assets are, and how they might be vulnerable to different lines of attack. That is the key value that the ForeScout platform brings to cybersecurity. By accurately identifying every facet of connected devices, it can provide a big force multiplier for any existing security plan. And that visibility extends to both the internet of things (IoT) and information technology's more blue-collar sibling, operational technology (OT).

ForeScout has been around for a long time, though they only recently pivoted and positioned their technology directly into the cybersecurity realm. Historically, most administrators probably recognize ForeScout as the makers of network access control (NAC) software. A secondary benefit to the ForeScout NAC platform was always a deep visibility into the devices that were being access controlled. Today, that is the main focus of the ForeScout cybersecurity platform.

The idea is that without good visibility, any cybersecurity program is going to have a difficult time dealing with permissions and weeding out legitimate threats from common false positives. ForeScout focuses on visibility first, and from that is able to natively provide asset management and compliance. By applying a security policy engine and partnering with other vendors, ForeScout can additionally provide network access control, network segmentation and a speedy or even automatic incident response capability.

John Breeden II/IDG

A helpful addition to the main interface, ForeScout provides a graphical view showing how created policies will trigger, and what kinds of devices will be affected.

ForeScout is installed in two main parts, an enterprise manager that houses the main user interface, and a scalable appliance that collects information about the various endpoints and devices being monitored. The appliances can be physical or virtual, and are designed to be installed dynamically however is most convenient for customers. For example, one could be placed at every branch office, or within a main data center, or whatever provides the most access to network resources. There is no limit on how many appliances the enterprise manager can track, and no agents ever need to be installed on endpoints.

Users can also install network traps to collect data about devices connecting to a network. These can be part of the ForeScout installation if an organization needs it, or ForeScout can simply integrate with any existing traps if another network traffic or cybersecurity platform has installed them. Pricing for ForeScout is based on the number of endpoints being protected.

Testing ForeScout

Once ForeScout was installed, it was able to instantly recognize whenever a new device was connected to the testbed network. It has access to a large number of sources, both passive and active, for clarifying and classifying anything that connects to a protected network. These include things like the SNMP traps, Radius requests, TCP fingerprinting, a MAC classification database, Power over Ethernet settings, DHCP fingerprinting, NetFlow, integration with VMware vSphere and many others on the passive side. For active profiling, it can use Nmap, WMI, SSH, RPC, SNMP queries to endpoints, or several other protocols.

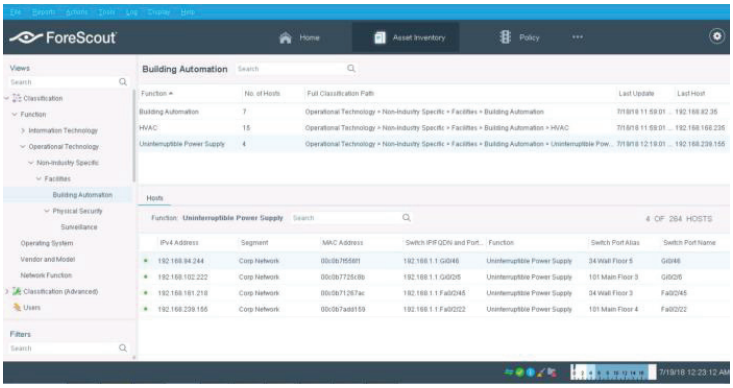
It's important to note that the administrators of ForeScout can decide what kind of scanning to use in which parts of the network. This is critical in OT environments where active profiling could potentially trigger industrial control devices, especially non-intelligent ones with limited functionality. By setting up passive-only profiling in those areas, ForeScout can avoid any

John Breeden II/IDG

While much of the work within ForeScout is done inside the policy engine, ForeScout's highly customizable web dashboard can keep users apprised of any issues that pop up, or new devices trying to connect to the network.

chance of interfering with OT operations.

Once profiled, ForeScout provides extremely detailed information about each device. Within the enterprise manager, users can see if a device is part of the OT or IT environment, what operating system is being used, the vendor's name and also the model number. For example, ForeScout was able to identify an IoT surveillance camera within the testbed as well as a lighting controller that was technically an OT device. It also told us about a smartphone connecting wirelessly, down to the type of phone it was, and the version of the operating system.

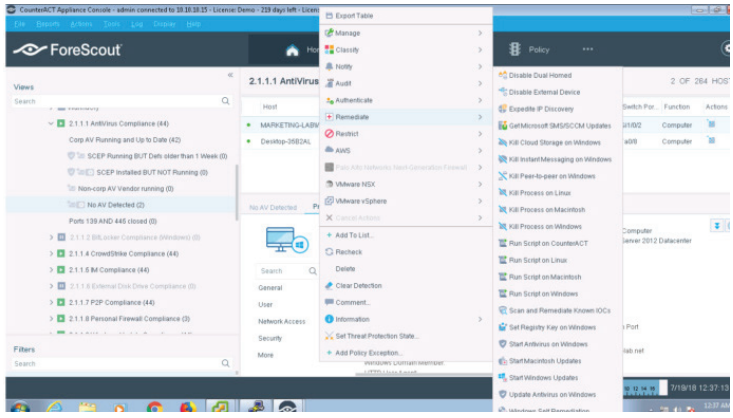


John Breeden II/IDG

ForeScout is one of a very few programs that can help to track and manage operational technology alongside of information technology. Everything from lighting controllers to HVAC units can be discovered and managed.

The ForeScout platform has access to a database of over five million device profiles, which is how it identifies so many of them. During our testing, there was one instance where it was unable to fully profile a device, which happened to be a brand-new IP phone. In that case, it went into an uncategorized bucket. At that point, we were given as much information about the unknown as it could collect, and were asked if we wanted to self-identify it. Once we did, the ForeScout platform was able to identify that brand and model of IP phones whenever they connected in the future.

That fixed the unknown problem locally, but we also had the option of uploading our self-assessment to the ForeScout cloud. Whenever a customer does that, it's sent to a team of experts who verify that the profile was properly assigned, and then share it with the rest of the community, expanding the profile database. That way the profile database is constantly growing, and the next customer who plugs in the same model of IP phone will have ForeScout fully identify it for them from the start. The sharing process is completely optional, though doing so helps the overall community of users.

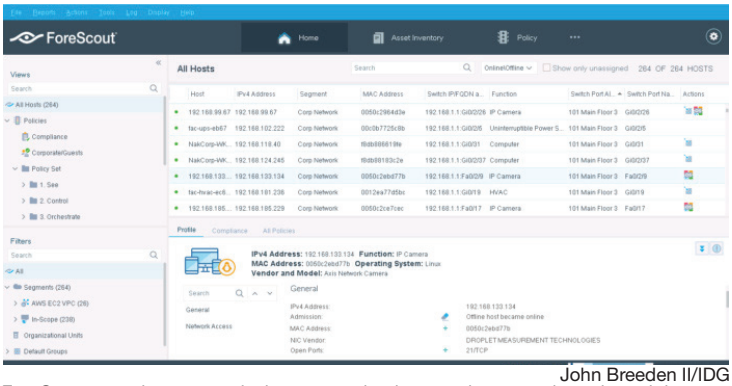


John Breeden II/IDG

Because ForeScout can interface with most cybersecurity hardware and software platforms, users can remediate most threats or potential threats right from the main ForeScout console.

Armed with detailed profiles, ForeScout users can set policies for various devices, and enforce them through the platform. Because ForeScout interfaces with everything from Splunk to Check Point to Palo Alto Network switches as well as many other devices, entering policy information into ForeScout and having it automatically program security devices is likely a lot easier than, say, trying to program network firewalls by hand.

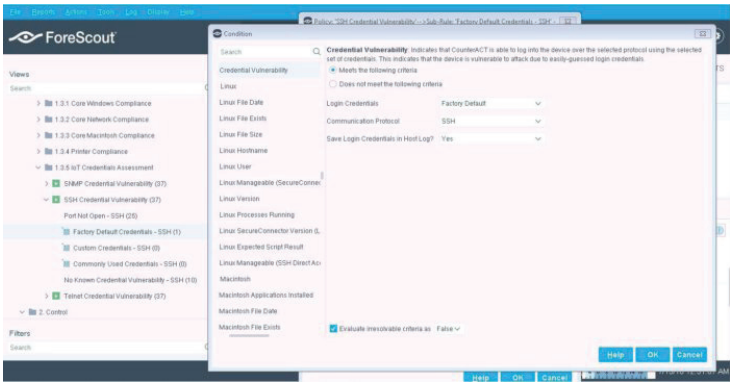
ForeScout comes pre-loaded with quite a few security profile templates based on best practices. They can all be edited, which saves time over trying to create a bunch of new profiles from scratch. They can be extremely simple, such as not allowing unknown devices to interface with a network until they are identified, to extremely complex, such as only allowing certain devices to use specific network resources, and only in specified ways such as when connected using a wired interface.



John Breeden II/IDG

ForeScout can show every device connecting in an entire network, and sort it in a variety of ways to help set more relevant security policies.

The policy engine can be an extremely powerful tool for dealing with new kinds of devices, such as IoT, and ensuring that nothing slips under the radar. During our testing, we used a default policy to query every new IoT device that connected to the network to see if it still had either its known factory default password, or something simple like "admin" or "password." If it did, access to the network was restricted, and the administrator for that device was notified. Once the password was changed, ForeScout automatically let it begin using the network according to other IoT policies we set for compliant devices.



John Breeden II/IDG

Many IoT devices are tiny, unmanaged, and create network vulnerabilities that attackers can exploit. The ForeScout platform enables administrators to detect and manage IoT as it shows up on a network, even checking to see if devices are open to known vulnerabilities or have factory-default passwords.

The ForeScout platform can also be set to report into network help desks. Doing this would enable help desk personnel to know exactly why a user is being denied access to network resources whenever they called in, assuming it's ForeScout that is doing the blocking.

The core of the ForeScout platform is deep visibility into any device. That makes for a powerful tool, but layering on a policy engine and tightly integrating it with almost any other network security program makes ForeScout even more useful. The information it provides can improve almost any other cybersecurity defense, and including IoT and OT under the same security blanket is just icing on the cake for this impressive, easy-to-use platform.