Device Discovery for Vulnerability Assessment: Automating the Handoff

OVERVIEW

While vulnerability assessment tools are widely believed to be very mature and approaching commodity status, they are only able to scan and analyze those assets they know about. In this white paper, we'll highlight how automating both device discovery and making VA tools aware of new devices that should be scanned can enforce security policies, increase the ROI of vulnerability scanning investments, and strengthen an organization's overall security posture.

Table of Contents

Vulnerability Assessment Tools: A Market Overview

In his August 2017 post, Gartner Analyst Augusto Barros succinctly summed up the strengths and weaknesses he saw in the Vulnerability Assessment Tool market:

> Vulnerability assessment is usually seen as a boring topic and most people think the scanners are all equal – reaching the "commodity" status. Well, for basic scanning capabilities, that's certainly true. But vulnerability scanners need to stay current with the evolution of IT environments; think all the changes in corporate networks in the past 20 years due to virtualization, mobility, cloud, containers and others. Those things certainly affect vulnerability management programs and how we scan for vulnerabilities. These IT changes force scanners to adapt, and we end up seeing some interesting differences at the fringes.

In "A Comparison of Vulnerability and Security Configuration Assessment Solutions", the analyst firm looks at the 5 leading vendors (BeyondTrust, Qualys, Rapid7, Tenable and Tripwire) to show how each tool differs in categories like:

- Agent-based scanning
- Integration with virtualization platforms
- Integration with IaaS cloud providers
- Mobile devices vulnerability assessment capabilities
- VA on containers
- Delivery models (on-prem, SaaS)

In all cases, the underlying challenge is the fact that our compute environments have become fragmented with multiple device types that the vulnerability tools must know about. And while the efficacy of the 5 leaders is taken for granted, the ability for each to find, understand, and scan each device remains a limiting factor.

Why are VA Tools Important?

It's probably fairly obvious to readers that vulnerability assessment tools are useful to organizations concerned about security. As far back as 2014, NetworkWorld[1] described the value as:

> Vulnerability scanners can help you automate security auditing and can play a crucial part in your IT security. They can scan your network and websites for up to thousands of different security risks, producing a prioritized list of those you should patch, describe the vulnerabilities, and give steps on how to remediate them. Some can even automate the patching process.

In short, vulnerability scanners may be the most trusted and common form of automated security products. They are able to constantly scan an organization's environment to find assets that need updating, are frequently updated with newly found vulnerabilities, and can often automate patching.

In addition to the functional value they provide, many industries require compliance with regulations that require vulnerability management. A few examples:

- **PCI/DSS** – The Payment Card Industry Security Standard requirement 11.2 states that organizations are required to "run internal and external network vulnerability scans at least quarterly and after any significant change in the network." In addition, the requirement specifies approved scanning vendors (ASVs).
- **HIPAA** - Strictly speaking, the HIPAA regulations do not have a specific standard or requirement for vulnerability scanning but require a risk analysis of covered entities to understand and document the risks to patient health data. In addition, NIST has issued a special recommendation for HIPAA that says, "Conduct trusted penetration testing of the effectiveness of security controls in place, if reasonable and appropriate. This validates your exposure to actual vulnerabilities."
- **GDPR** – The EU's General Data Protection Regulation (GDPR) which goes into effect on May 25, 2018 gives broad requirements like "prevent accidental or malicious incidents that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."

Again, these are just a few examples of regulations that require the automated vulnerability identification and remediation capabilities found in today's vulnerability scanning tools. There are more.

[1] 6 free network vulnerability scanners, NetworkWorld

Visibility and Vulnerability Assessment Tools

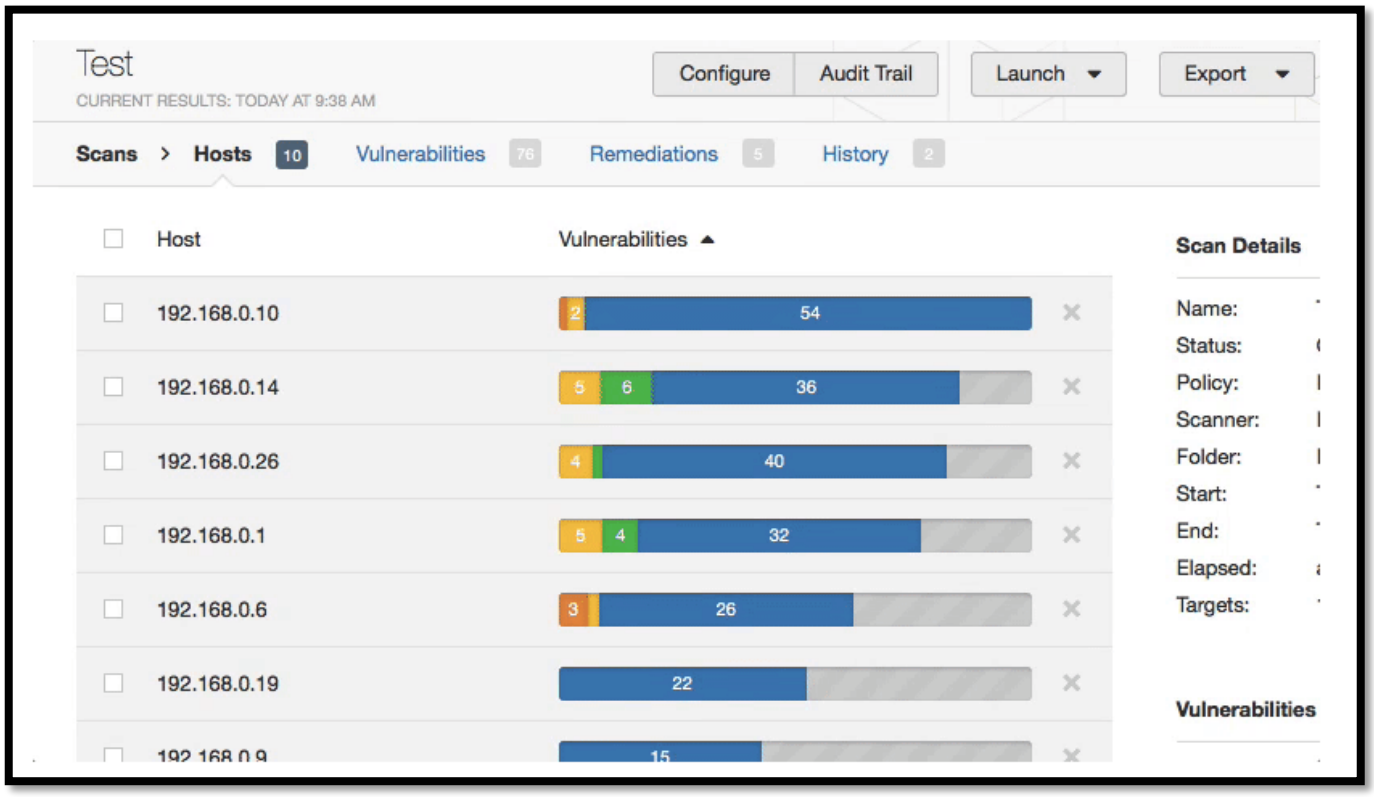
When we think of the term “visibility” and how it relates to VA tools, we’re really considering two things:

1. What device information the VA tool is able to see
2. What level of visibility of the overall device environment we get as a result of VA scans

WHAT CAN VA TOOLS SEE?

At the most basic level, VA tools need only to see the version of installed software on devices in order to produce a prioritized list of devices that should be patched. Given the installed software on devices, these tools are able to compare against their dynamic list of known vulnerabilities for each software version.

Example Vulnerability Assessment Report



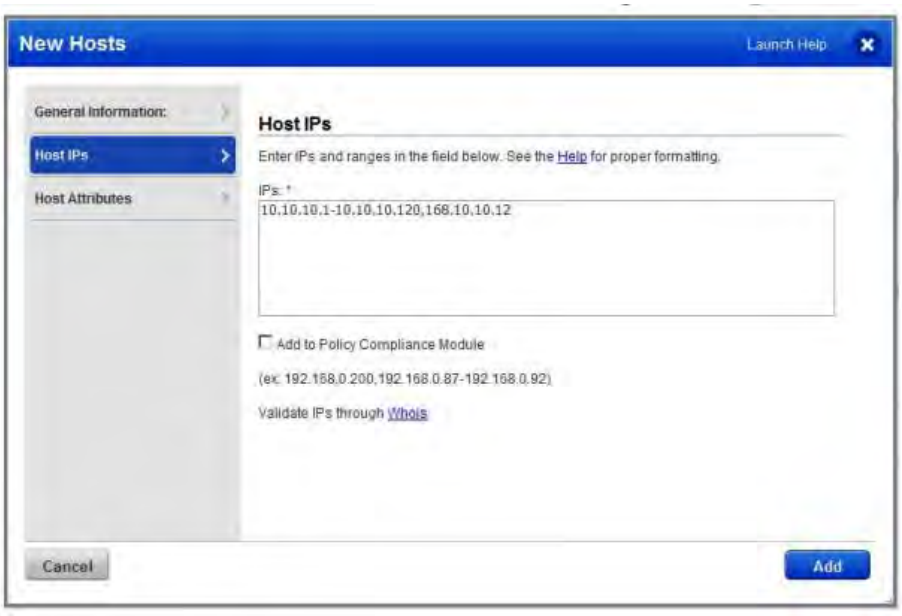
WHAT LEVEL OF VISIBILITY DO VA TOOLS PROVIDE?

While a prioritized list of IP addresses and their associated vulnerabilities is helpful in planning a patch management initiative, using VA results for device visibility presents significant shortcomings:

1. Device Discovery
2. Device Type Support
3. Policy Validation

Device Discovery with Vulnerability Assessment Tools

While vulnerability assessment tools exist to, and excel at scanning known devices for known vulnerabilities, they can only scan those devices they are aware of. In many cases, these tools require manual entry of device information including IP addresses. In a very small organization, manual entry of device info may not be an issue. However, in a multinational, distributed environment, this can't scale.



Adding New Hosts to a VA Scanner

To be clear, device discovery was never the intended functionality of VA products. Just as we don't expect antivirus tools to detect new devices, we cannot criticize VA tools for lacking device discovery capabilities. However, the need to bridge the gap between newly discovered devices and the VA tools trusted to know the resident vulnerabilities is a common, acute issue.

Device Type Support with Vulnerability Scanners

The fragmented and dynamic nature of today's computing environment presents several challenges when it comes to device discovery:

- **Cloud and Virtual Machines** – The relative ease and speed of spinning up virtual instances can lead to several live instances of machines not known by VA tools.
- **IoT Devices** – The explosion in the number of always-on, always-connected smart devices with different OS flavors represents another challenge to VA scanners.
- **Mobile** – As mentioned in the Gartner report, the different VA tools profiled offer differing levels of support for mobile devices.

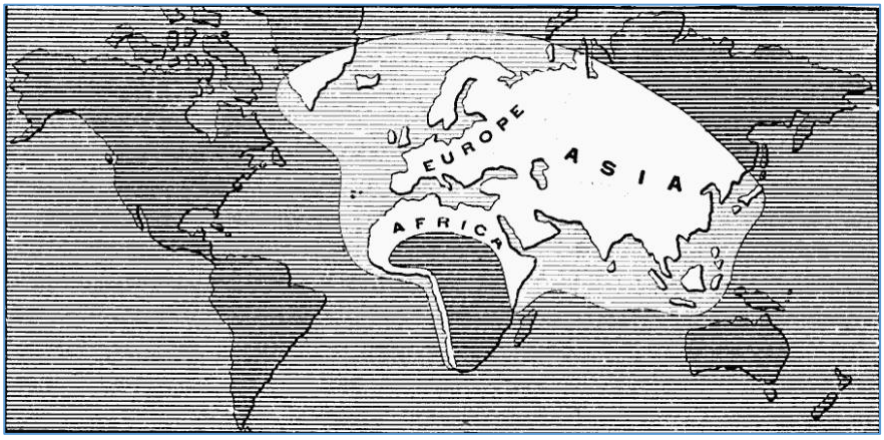
While these tools do a fantastic job identifying potential vulnerabilities, they can only do so on the devices they can see and support.

Policy Validation with Vulnerability Scanners

Finally, VA tools have no contextual awareness of an organization's security policy, but instead act as the facilitator and execution arm of the policy. Rather than knowing that all devices should be scanned by the VA tool, these products know only to scan anything they scan see (as long as the device is supported).

The result is a complete picture of the environment that a VA scanner is aware of, but without analysis of unknown, unmanaged, and unsupported devices that are required to be scanned as part of the overall security policy.

Using the results of a vulnerability scan as a proxy for full device visibility is like looking at a map of the known world in the time of Columbus. *We know what we know, and we don't know what we don't.*



Automating Device Discovery

So far, we've hopefully made 4 points clear:

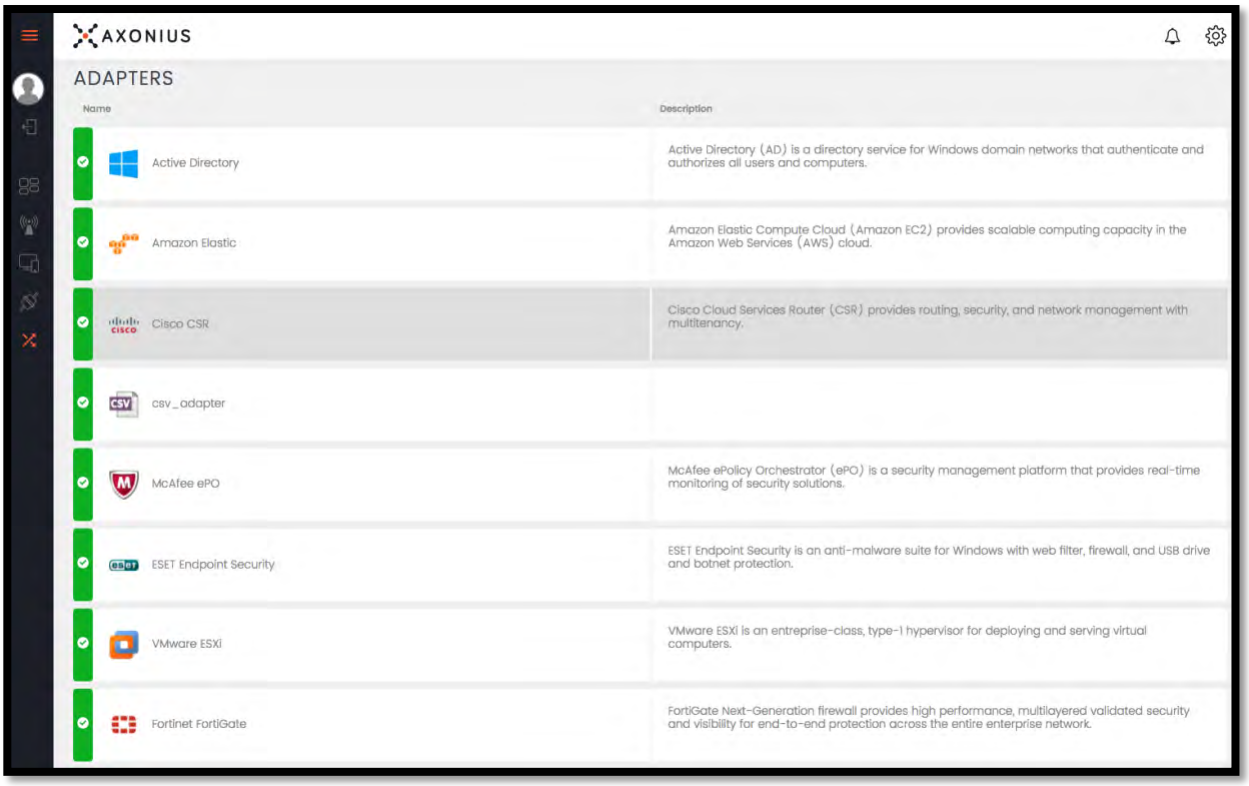
1. VA tools are exceptionally useful at finding known vulnerabilities.
2. The results of a vulnerability scan can effectively prioritize a patch management strategy.
3. Vulnerability scanners can only scan those devices they know exist.
4. Using VA scan results for full device visibility is not the intended use and presents limitations.

Let's take a look at how to bridge the gap between device discovery, the handoff to VA tools, and how to gain full visibility into the state of each device to see and secure all.

Connecting to Devices Through Management Systems

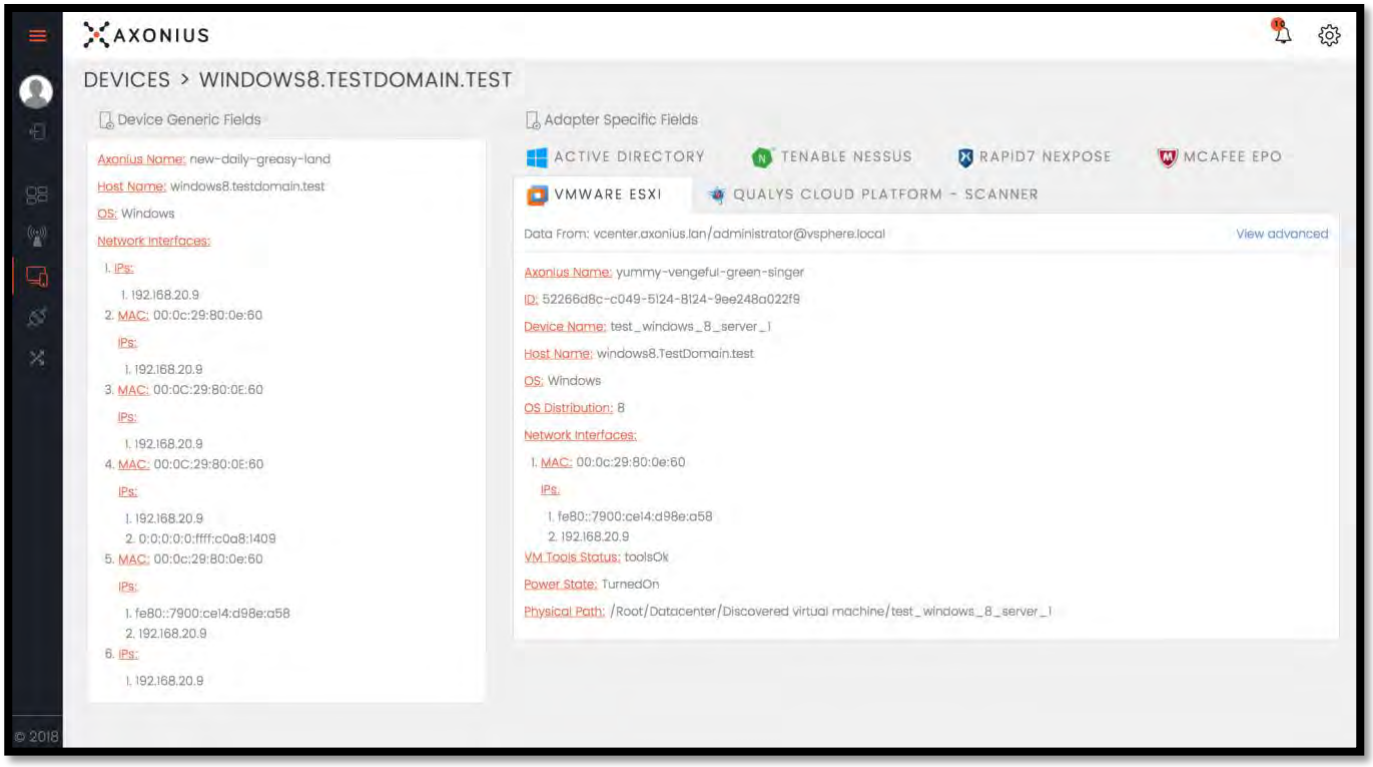
Organizations already have multiple systems that manage things like identity and access, endpoint protection, network-based security, patch management, mobile device management, and the list goes on. There are many systems, each knowing different pieces of the device puzzle, but there's no way to get a universal view to cross-correlate and ask interesting questions.

Using adapters, the Axonius platform is able to connect to each of these systems to gather data about the state of each device:



Correlating Data to Create a Unique Device Fingerprint

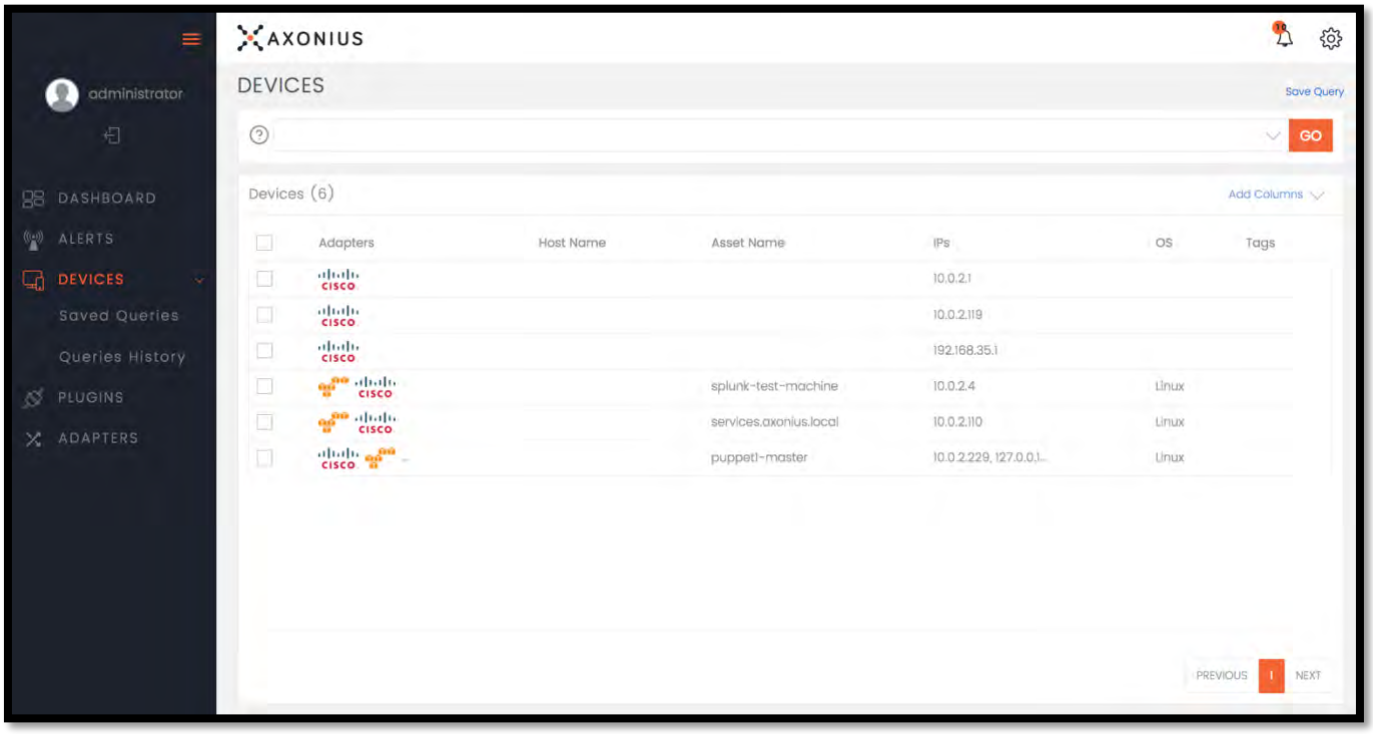
Once connected to the devices and management systems in a customer's environment, adapters create an abstraction layer to the devices to get a single view of what's known about all devices.



A look at a single device through the lens of multiple management systems

Discovering New Devices

As the Axonius platform is able to see all devices, it is able to see anything new in a customer's environment and can make a determination as to whether that device is already managed. For example, if a customer is using a VA tool and the policy states that everything must be scanned, Axonius can see all new devices that have hit a Cisco switch but aren't known to a VA tool.

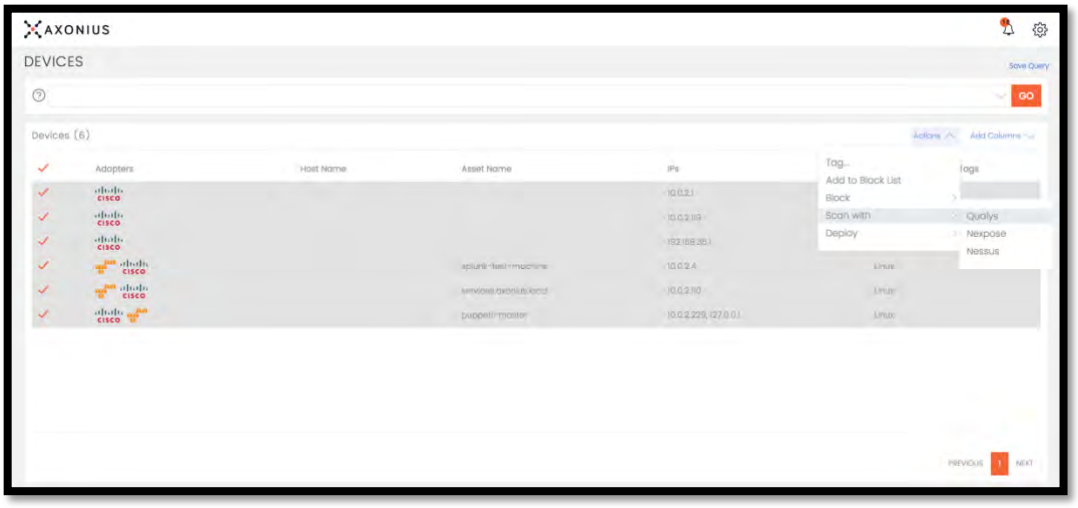


Show all unmanaged devices in Axonius.

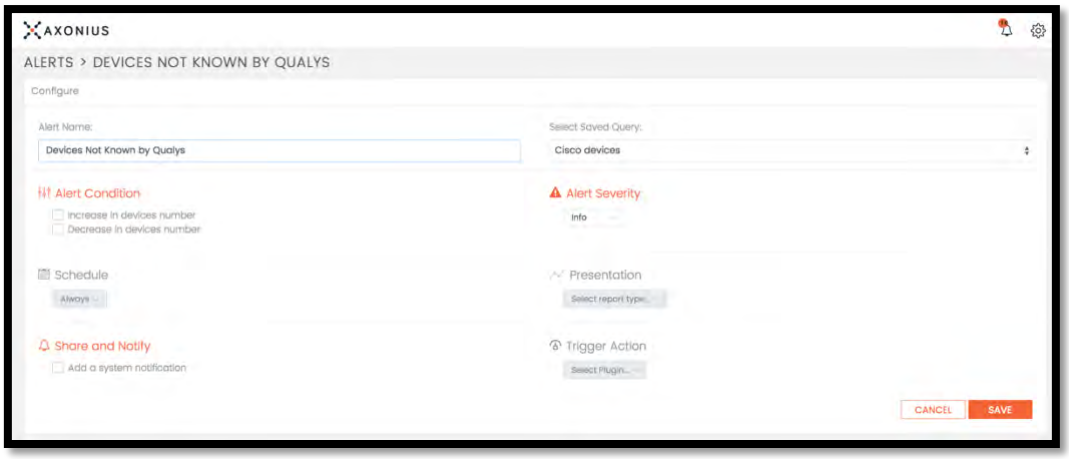
Informing VA Tools of New Devices

Taking the example a step ahead, let's say we want to inform Qualys about these new devices to add them to the next scheduled scan.

Simply selecting the devices and clicking "Scan with > Qualys" will add those previously unknown devices to the next scheduled scan.

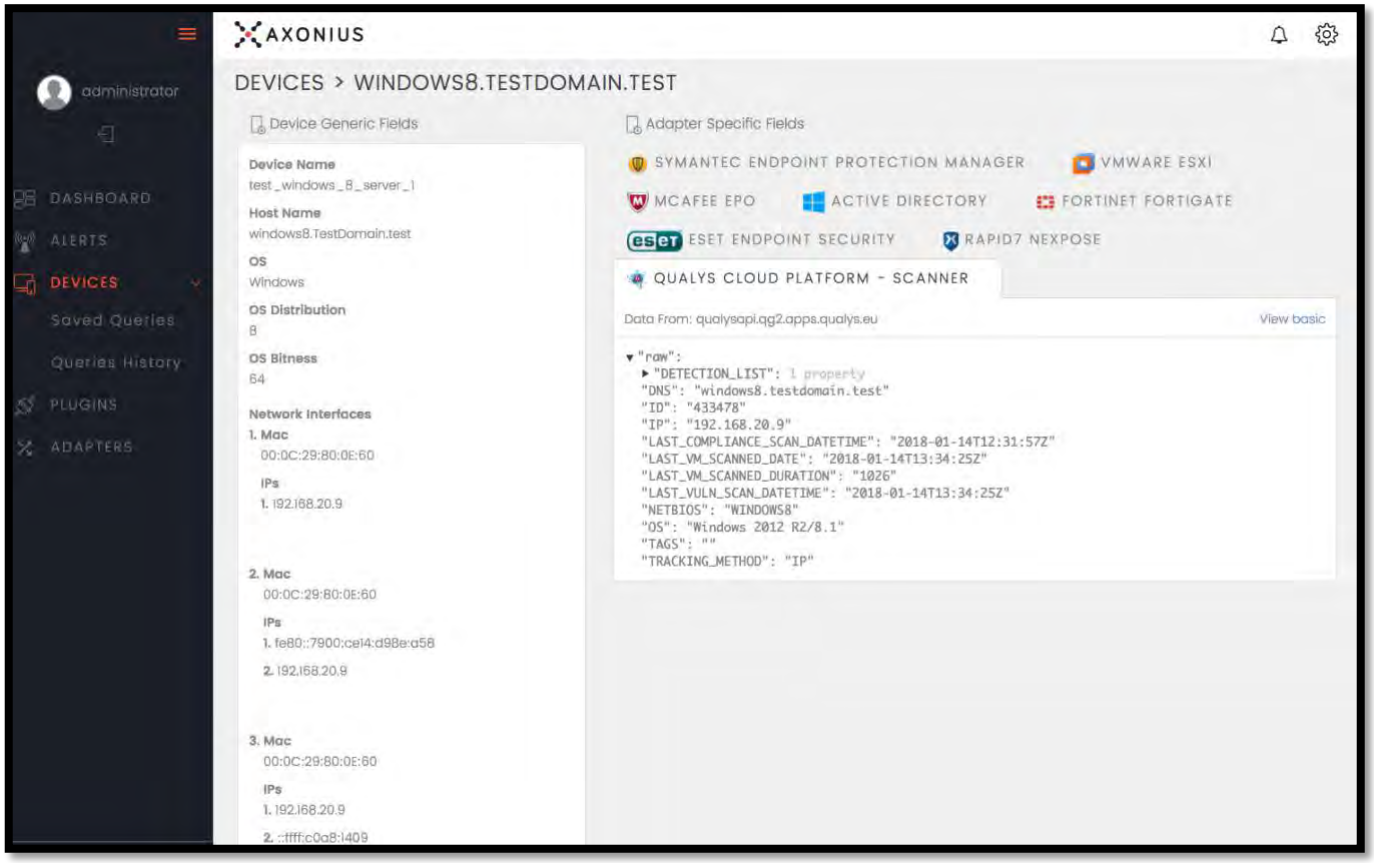


In addition, we can create an alert to show any time devices meet these criteria, and it can either be sent via email or syslog:



Automating the Handoff to VA Tools

Using the device discovery, correlation, and analysis capabilities of the Axonius Cyber Security Asset Management platform, we're now able to automate the end-to-end process of finding new devices and making sure that the vulnerability scanner is aware that it has new devices to scan.



By bridging the gap between device discovery and vulnerability scanner device awareness, we're able to validate adherence to the organizational security policy, knowing that all new devices will be scanned.

About Axonius

For organizations that see opportunity in today's always-on and always-connected reality, Axonius is the Cyber Security Asset Management (CSAM) platform that lets IT and Security teams see devices for what they are in order to manage and secure all. By easily integrating with customers' existing management and security technologies and using an extensible plugin infrastructure to add custom logic, customers are able to get a unified view of all devices – both known and unknown. Axonius aims to be IT's favorite Security tool and Security's favorite IT tool. For more information and to see what's possible with a universal view of all devices, visit Axonius.com.

Support and Questions

We are committed to helping our customers deploy, configure, and start seeing value immediately. The POC deployment process will be hands-on, with any and all support services available to get up and running. Should you have any questions, concerns, or product feedback, please do not hesitate to contact your Axonius account representative at any time.

Thank You

Finally, we want to thank you for considering working with Axonius. As IT and Security professionals ourselves, we understand the time and effort it takes to consider a new product. Thank you for trusting us to help you.