ARMIS NETWORK PERFORMANCE ANALYTICS

ARMIS NETWORK PERFORMANCE ANALYTICS

Network Analytics Redefined

As the number and diversity of endpoints coming onto enterprise networks increases, managing the network and troubleshooting network problems become increasingly complex. The range of devices includes managed endpoints, such as laptops, as well as unmanaged endpoints, such as cameras, inventory systems, healthcare devices, etc. And of course, every endpoint requires network services such as an IP address and DNS, and of course network capacity.

Unfortunately, traditional network management tools don't provide visibility into what each type of endpoint is doing or what problems it might be having. And traditional security tools have a hard time detecting when these different types of endpoints have been compromised in a simple and intuitive user interface console.

To help network managers efficiently deal with a wide range of users and endpoints and enhance wireless security and performance, Armis provides a wealth of information about the usage and health of your physical network, connected devices, and associated network services. These key performance metrics let you:

- Optimize your network infrastructure
- Troubleshoot various types of network problems
- Assist in traffic engineering as the network scales

Unlike traditional network management systems, Armis is able to provide information down to the granular level of an individual user, device, access point and radio, letting you visualize errors and data traffic conditions on a configurable time basis such as the last ten minutes or the last 30 days. And even better, all of the information Armis provides can be correlated to locations and endpoint types.

Below are several examples in which Armis helps network managers quickly solve problems.

Situation 1: End-user contacts the help desk complaining that the WiFi network is running slow.

Armis let you quickly see the historical data for a particular user. In this situation, Armis network analytics can determine the likely root causes of bad WiFi performance for this user.

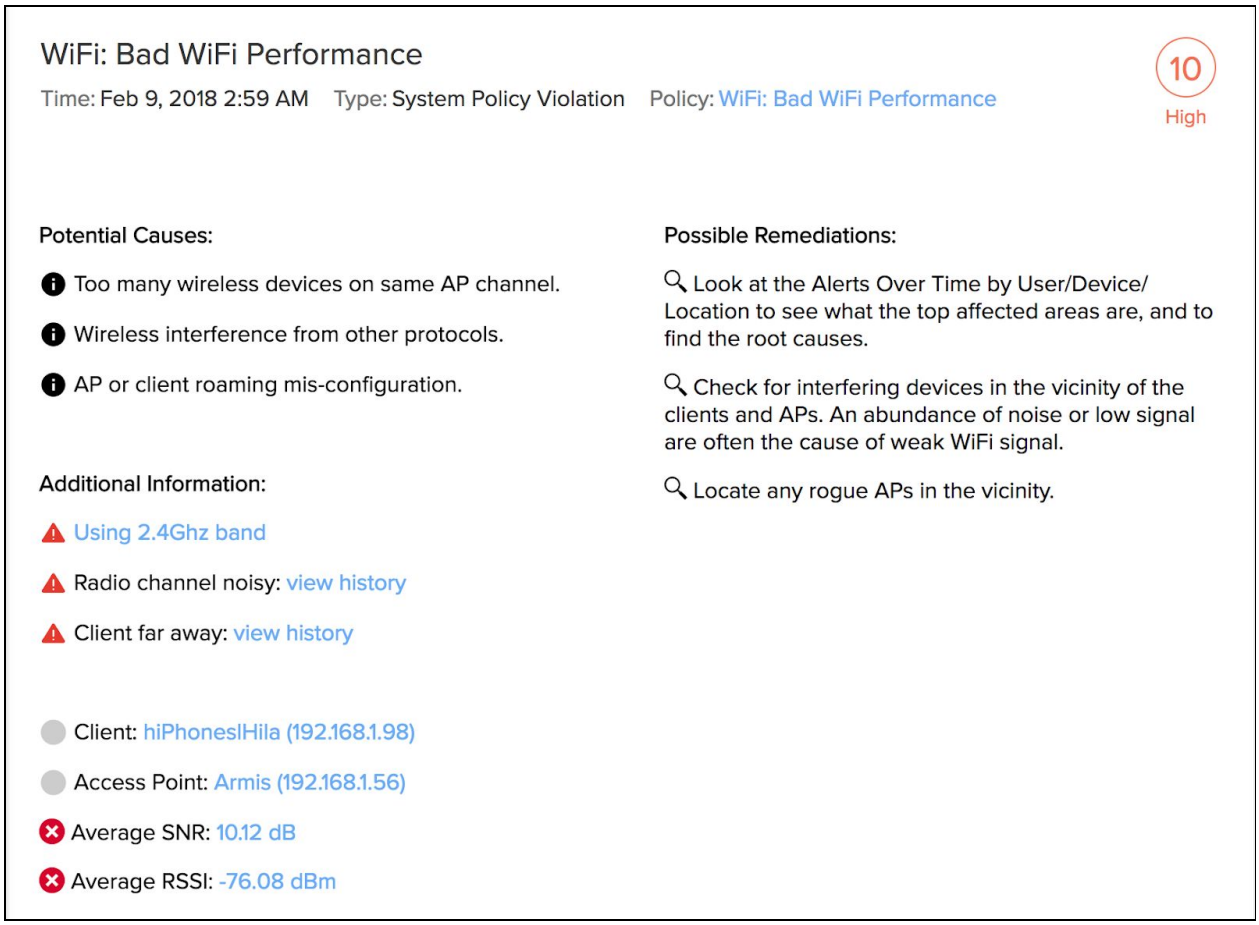

Figure 1: Armis network analytics provides root cause analysis for slow WiFi.

Situation 2: End-user complains that he can't access the Internet

In this situation, Armis network analytics can determine that the root cause was a DNS issue.

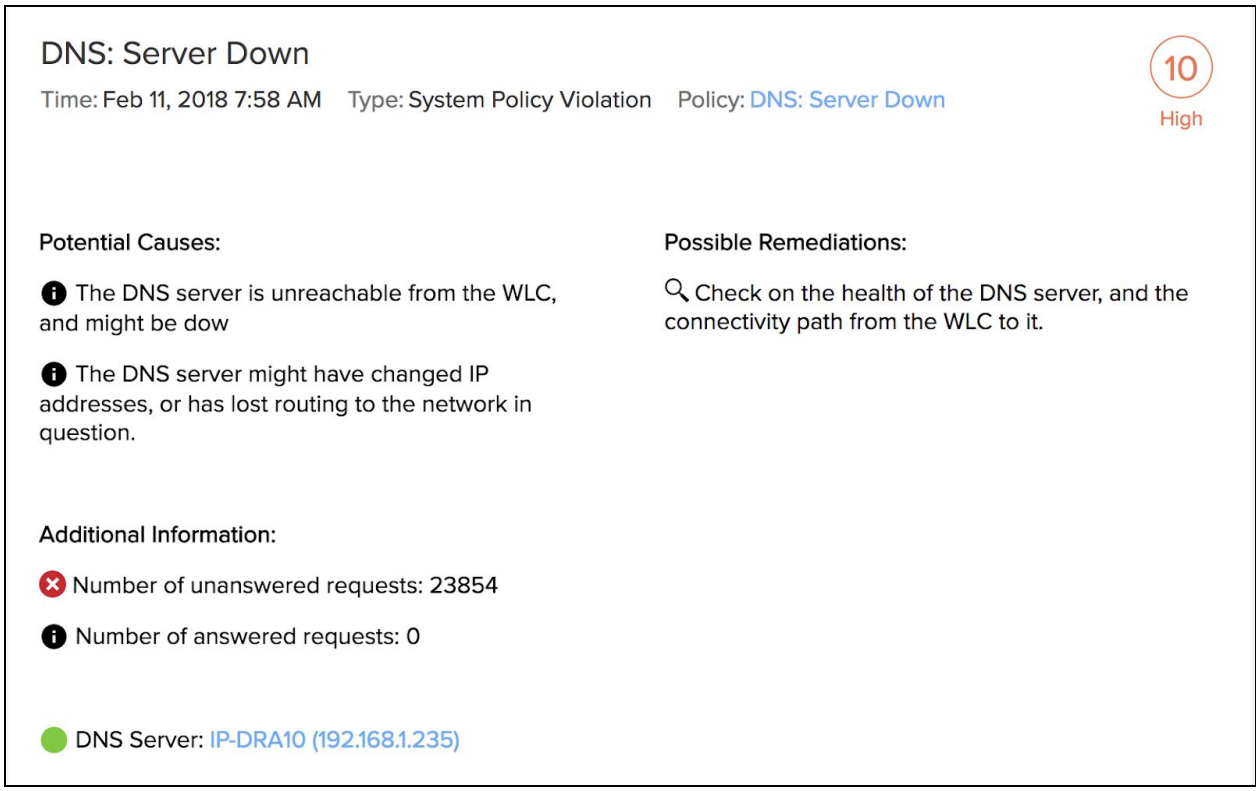

Figure 2: Armis network analytics provides root cause analysis for inability to access the Internet

Situation 3: Network capacity is insufficient

Network managers often need visibility into true network capacity. When you have too little capacity, users experience connectivity problems. When you have too much capacity, you have wasted money on unneeded access points.

Armis network analytics quickly shows you the access points that are over-utilized as well as those that are under-utilized.

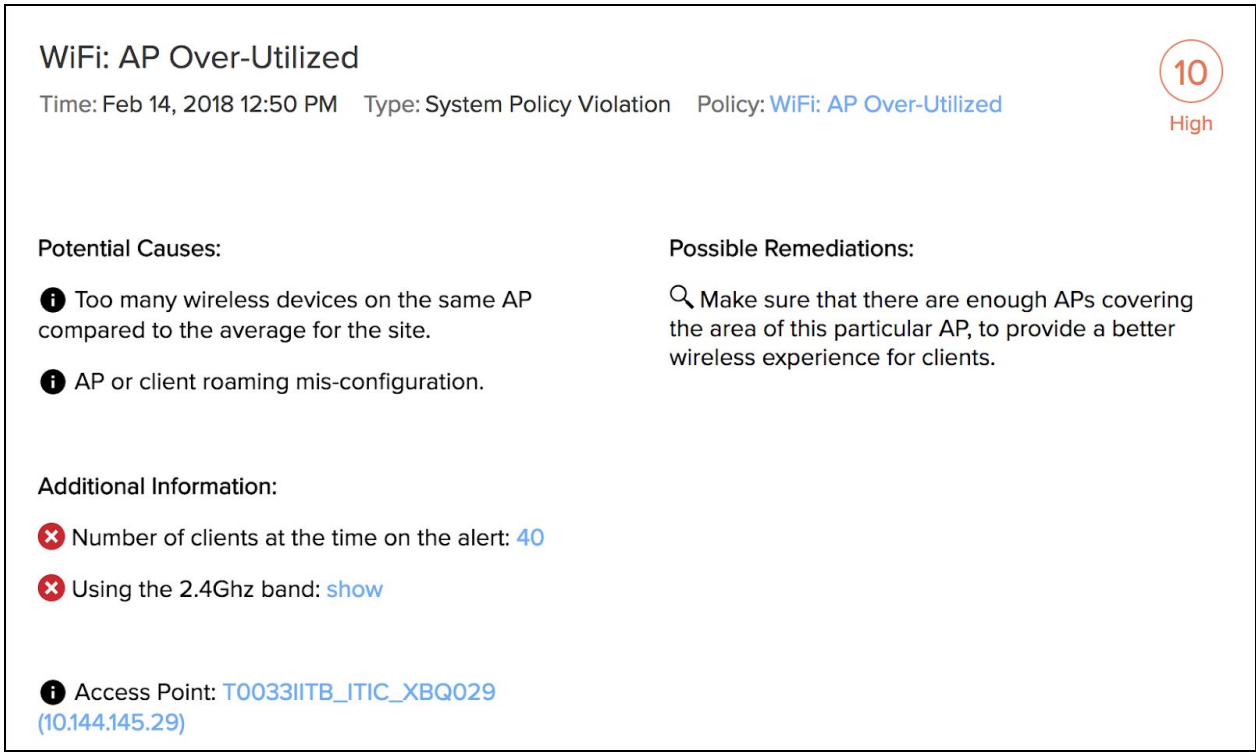

Figure 3: Armis network analytics tells you when access points over- or under-utilized.

Situation 4: Internal application performance is slow

When an end-user contacts the help desk complaining that internal applications appear to be running slow, Armis lets you see L1, L2, and L3 layer statistics and other possible root causes such as routing issues, severely overloaded website, and oversubscribed application.

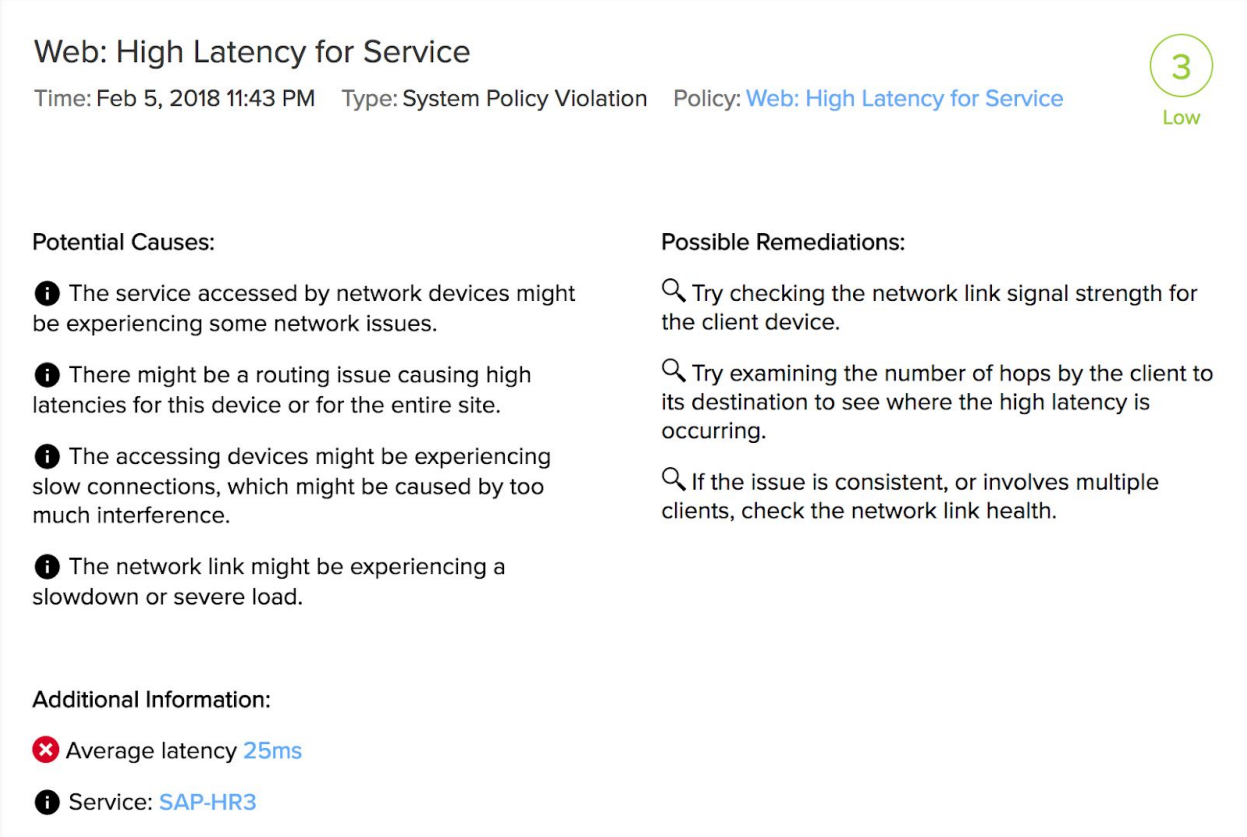

Figure 4: Armis network analytics provides root cause analysis of poor performance of internal applications.

Situation 5: Software trend analysis

Sometimes it is valuable to see how the incidence of applications or operating systems have trended over time. This may help you measure the success rate of a program to apply patches, or it may help you see how vulnerable your enterprise is to a new type of exploit.

Armis network analytics lets you see the number of systems that are utilizing different versions of applications over time.

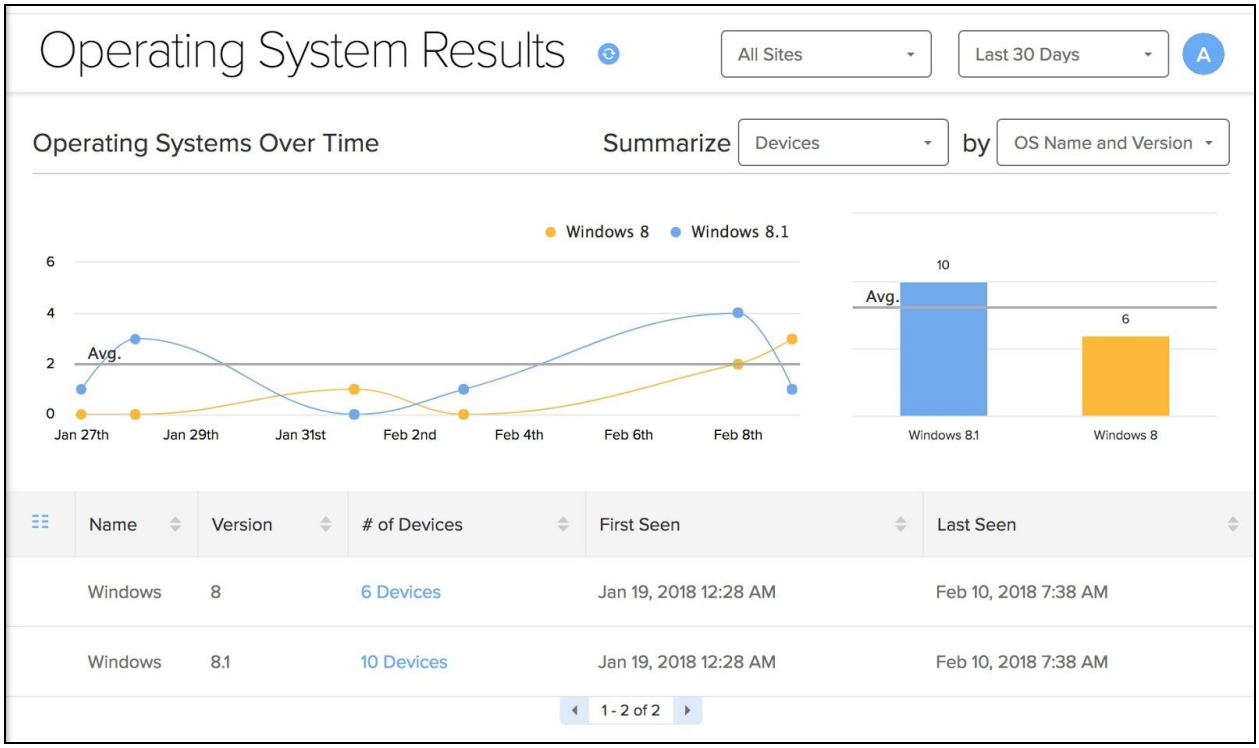

Figure 5: Armis network analytics provides a historical trend analysis of software running on the network.

Features List

The following are the network statistics and troubleshooting data that Armis gathers. All of these statistics are in addition to the vast amount of information that Armis gathers about devices as part of Armis' security analysis features.

- Latency
- Jitter
- Packet loss
- Server down
- RSSI
- SNR
- DHCP errors
- Weak WiFi signal for a client
- Authentication errors for a client
- Bad WLC to RADIUS server connectivity
- AP under utilized
- AP over utilized
- DNS performance

About Armis

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

20190527.1