For IT organizations, managing and securing networks is a dynamic challenge that is complicated by the myriad of devices that connect to the corporate networks. Mobile devices (laptops, smart phones, tablets, etc.) routinely access different networks from privileged corporate networks to free public WIFI Hotspots. MDM (Mobile Device Management) technologies are the preferred solutions used by Corporate IT to manage devices at scale and reduce the risk to vital corporate data assets.

However, with a highly mobile workforce, how does the IT operations team ensure that all of the managed devices in the organization indeed have the appropriate MDM components installed and have proper utilization rates? Oftentimes, not all devices with MDM installed are properly accounted for resulting in inaccurate licensing compliance.

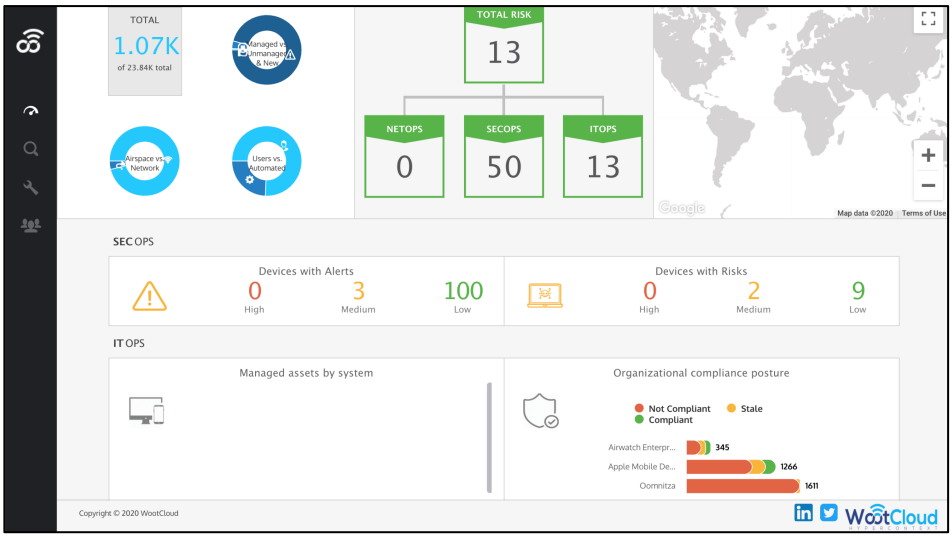

Figure 1 - WootCloud HyperContext Executive Dashboard

WootCloud HyperContext ™ addresses the discovery gap for most MDM systems from Jamf to VMWare's AirWatch. Using agentless technology, HyperContext -

- Discovers all devices on and around an IP network
- Creates fine-grained device context using multitude of attributes extracted from various sources like network traffic, integrations into enterprise components from active directory and asset management systems to EDR and vulnerability assessment software

Utilizing API integrations with MDM and SIEM technologies as well as network traffic analysis, HyperContext determines which unmanaged devices should be classified as managed devices and identifies ALL managed mobile devices not in compliance with the corporate MDM requirements.

Examining a situation that happens all too often in organizations, we present how WootCloud HyperContext assisted a Silicon Valley based hi-tech organization determine their compliance risk. The organization has over 23,000 devices identified, of which over 1,600 managed devices needed MDM implemented on them. It was also observed that 125 **unmanaged** devices had MDM installed which potentially triggers a licensing true-up.

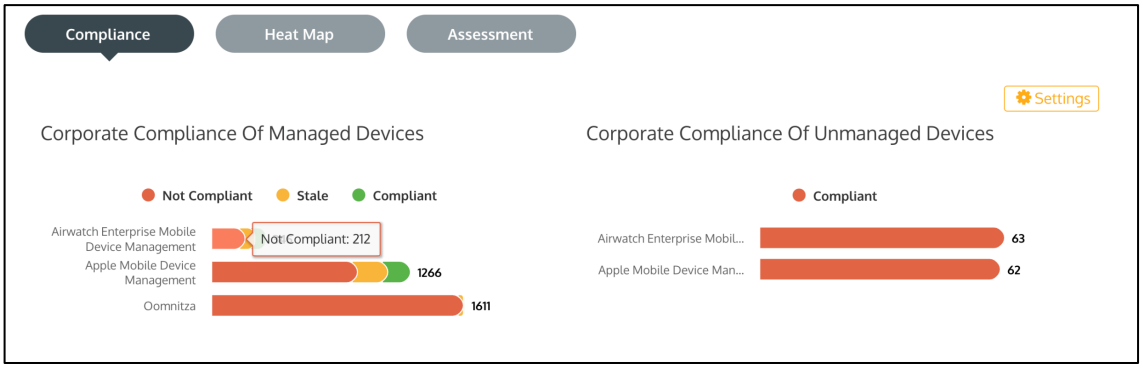

Figure 2 IT Operations Compliance Dashboard Highlight

Table 1 presents a breakdown of the managed devices.

Application	Not Compliant	Not Seen in > 15 Days (Static)	Compliant	Total
AirWatch Enterprise	212	64	69	345
Jamf	928	193	145	1,266
Total	**1,140 (71%)**	**257 (16%)**	**214 (13%)**	**1,611**

Table 1 Compliance State of Managed Devices

From this snapshot and analysis, it's clear that there is significant risk to the security posture of the organization with over **70% of the mobile devices not meeting the MDM compliance requirements** and yet granted unfettered access to the network.

With WootCloud HyperContext, this client was easily able to:

- Protect their corporate data by dynamically micro-segmenting their network at the device level
- Isolate non-compliant devices to a restricted network segment and
- Generate ITSM tickets simultaneously to install the MDM software on non-compliant devices

Once a device had the necessary software installed and became compliant, HyperContext automatically moved the device to the appropriate privileged network segment.

WootCloud HyperContext presents great value to organizations in many areas, including Asset Management, Compliance, Risk Assessment, real-time Threat Detection, network micro-segmentation, and more. In this use case, the focus is on Mobile Device Management, but the same principals can be applied in many other areas in such as IT Operations, Network Operations, and Security Operations. Not only did WootCloud uncover all devices that were non-compliant with the organization's MDM policies, but also helped our client determine the proper number of software licenses required for their environment.

For more information on how to easily implement WootCloud HyperContext to improve IT operational efficiency, visit www.wootcloud.com to schedule a demonstration today.