Defending the Educational Institution When Nobody is Around

With the ever-changing dynamics in the connected campus today, IT organizations are forced to be adaptable. There is a continuous influx of devices into the environment from visiting researchers, professors, and students. From Smart TV's to headless monitoring devices that do not traditionally have input/output peripherals such as a mouse, keyboard or display attached; these devices on your network are most vulnerable because they do not have the compute capability to run a security agent, thus rendering them susceptible to hacking attacks that will not be noticed immediately. So how, then, can we protect headless devices in colleges & universities today?

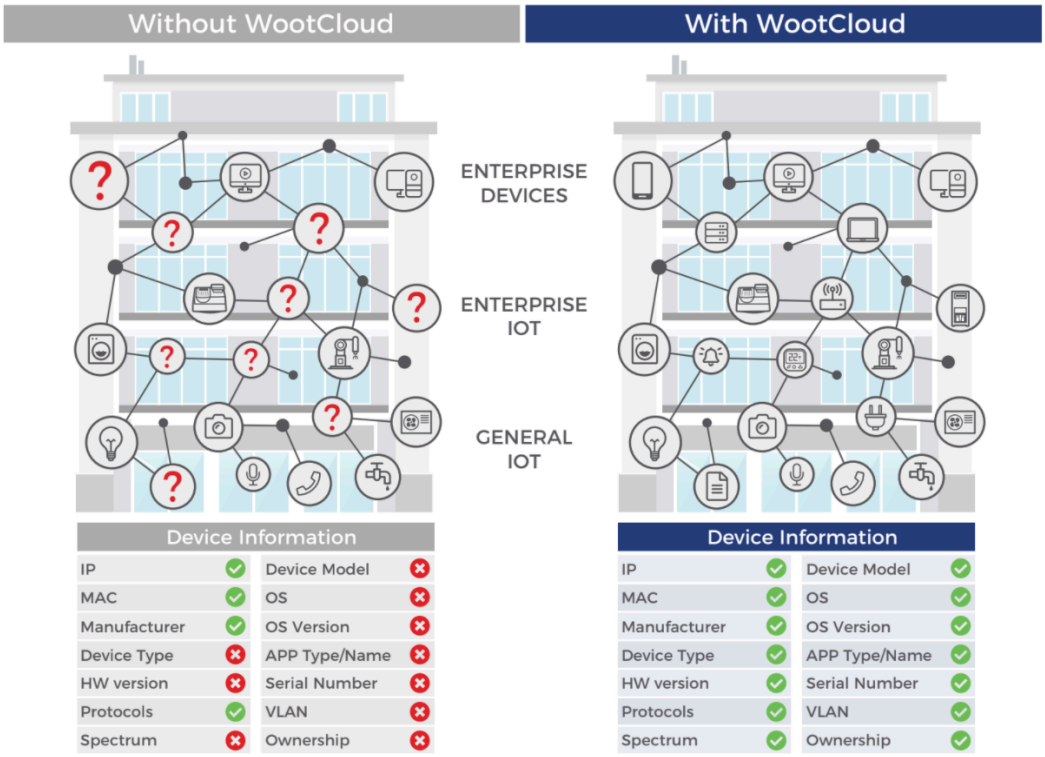
Expanded Attack Surface

Hackers have used headless devices to gain access to university resources for a long time. (Article: CSO Online) Student records, as well as critical research data are continuously viewed as high value targets by hackers. Even well-staffed security organizations cannot detect these security breaches (the average time of discovering breaches is 192 days).

WootCloud HyperContext technology

With our technology you can protect all your user-controlled and headless devices by scanning both the radio and network spectrum, gather hundreds of device parameters to automate network segmentation and automatically set nuanced granular policies at scale. You can also tailor security settings and create dynamic access control policies for all devices at IoT scale.

Get end to end device visibility and device contextual details with WootCloud HyperContext.



Download our full functioning Virtual Machine and start defending your defenseless medical equipment today. Contact us at getstarted@wootcloud.com or visit us at: www.wootcloud.com to learn more