Defending the Defenseless When Nobody is Around

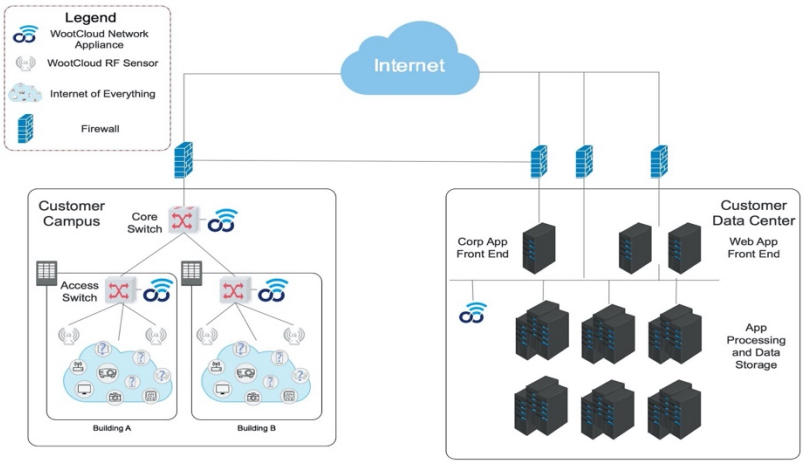
With the ever-changing dynamics in the connected workplace today, IT organizations are forced to adapt to a new normal of IT operations and cybersecurity. There is a continuous influx of devices into the environment. Whether it is new infrastructure equipment, or consumer IoT devices being used to gain access to corporate networks, or headless business devices that do not traditionally have an assigned user to manage them. IT organizations need to adapt to these dynamics to provide unfettered access to the appropriate business-critical information within the organization's network. From Smart TV's to Wireless Access Points, the most vulnerable devices on your network have no compute capability to run a security agent, rendering them susceptible to hacking attacks that will not be noticed immediately.

Expanded Attack Surface

Hackers have used headless devices to gain access to corporate resources for a long time. An example of this is WootCloud's discovery of botnets exploiting Polycom HDX devices and eavesdropping into corporate board rooms globally. Even well-staffed security organizations cannot detect these security breaches (the average time of discovering breaches is 192 days).

Adding ***WootCloud HyperContext***™ into the IT infrastructure dramatically enhances the ability to defend headless devices, even when nobody is around. The HyperContext platform leverages its advanced deep learning AI engine that enables the discovery and profiling of all devices in an agentless manner to eliminate threats to your headless devices at machine speed and at IoT scale.

Download our full functioning Virtual Machine and start defending the defenseless when nobody is around.



For more information, go to: www.wootcloud.com or send a request to sales@wootcloud.com

3031 Tisch Way
Suite 308
San Jose, CA 95128
T: 408-564-4220
sales@wootcloud.com