WootCloud
HYPERCONTEXT

WootCloud has domain expertise to combat flaws in IoT device security

IoT security is a growing concern today and the recent warnings from the FBI and other agencies reinforces the urgency of the situation.

FBI recommends that you keep your IoT devices on a separate network
Is your smart TV spying on you? A new FBI warning says it's possible
Securing the Internet of Things

The number of high-profile breaches covered in the press only scratch the surface of the problem. For every incident detected, there are many more that remain hidden, undisclosed or even go unrecognized. Traditional security solutions do not address the new security challenges posed by the variety of IoT devices and the solutions to these problems as presented in FBI articles, though accurate and simplistic, do not work for enterprises that deal with these devices at scale.

Looking deeper into the Internet of Things, and deployments of connected smart devices in healthcare, enterprise and most other verticals, WootCloud's own research reveals a common thread of problems. These are:

- Device manufacturers have very little background in dealing with security, and there are no security standards driving trusted software development on IoT devices.
- In many cases these devices have limited compute, memory and bandwidth and thus need an agentless solution as endpoint security solutions cannot be deployed on them.
- Many of these devices store and send sensitive data, including credentials, in plain text.
- The default configurations and passwords are public information. Customers deploying these devices in many cases continue to use the default credentials.
- Devices are interconnected over LAN, WAN and PAN. A Single attack can affect the entire series of connected devices.
- Due to the complex layers of the system, it's hard to identify where any one problem is originating.
- The devices occupy multiple communication spectrums like WiFi, Bluetooth, BLE and ZigBee.

WootCloud has detected active exploits of these problems at multiple enterprises and our research is available at WootCloud Threat Labs.

To solve these problems, WootCloud's agentless AI driven HyperContext™ platform provides contextualized device visibility to correctly and automatically profile each device and its behavior to set automated controls and identify threats that current device fingerprinting and security solutions cannot.   This HyperContext platform is a comprehensive enterprise standard platform that offers the following:

1. **HyperContext**: Identify automatically each and every device in and around network and understand its usage, risk and threat context. Learn more
2. **Micro-Segmentation**: Dynamically micro segment devices based on their context and micro-location. This decouples segmentation from the broken user authentication and L2-L3 based ACLs. Now devices can be grouped beyond IP, mac to offer micro-segmentation at scale. Learn more
3. **Dynamic Control:** Dynamically control access that these devices and users have, to other resources in the network based on context and real time threat assessment. No static ACLs but current device context drives enforcement dynamically. Learn more
4. **Automation:** Automation to handle devices at IoT scale via a policy engine driven by a strong understanding of the enterprises business requirements. Learn more

If you'd like a Demo of Wootcloud's Micro Segmentation abilities, please contact our team at sales@wootcloud.com

You can also enjoy a complimentary smart device survey for your organization.