EDUCATION SOLUTION BRIEF

WootCloud
HYPERCONTEXT

Context Driven Network Security for Connected Students

WootCloud HyperContext® is an unmatched device first solution, that provides contextualized visibility on all devices, their behavior, network access and threat intelligence, and uses this contextual intelligence to segment the network down to the device level, correlate threats and vulnerability propagation across multiple interfaces including RF and Networks, and automate access control at IoT scale.

HyperContext® recognizes anomalous behavior at the device level and uses the sophisticated policy engine to prevent vulnerable devices from propagating into the rest of the organization. Using HyperContext there is continuous dynamic network segmentation at the device level that extends beyond simple device identification. Based on our Telemetry, WootCloud customers have seen threat hunting time reduced by 70%, operational efficiency gains of 60% and improved segmentation time by 300%.

100% DEVICE DETECTION SCANNING MULTIPLE SPECTRA

WootCloud scans multiple communication protocols like WIFI, Bluetooth and BLE, and looks for devices both on and off the network, including the RF spectra. Other solutions only see devices connected or paired to the network. If the device emits an RF frequency, WootCloud can see it, fingerprint it, and categorize the risk to the rest of the network along with providing recommended actions.

CHALLENGES

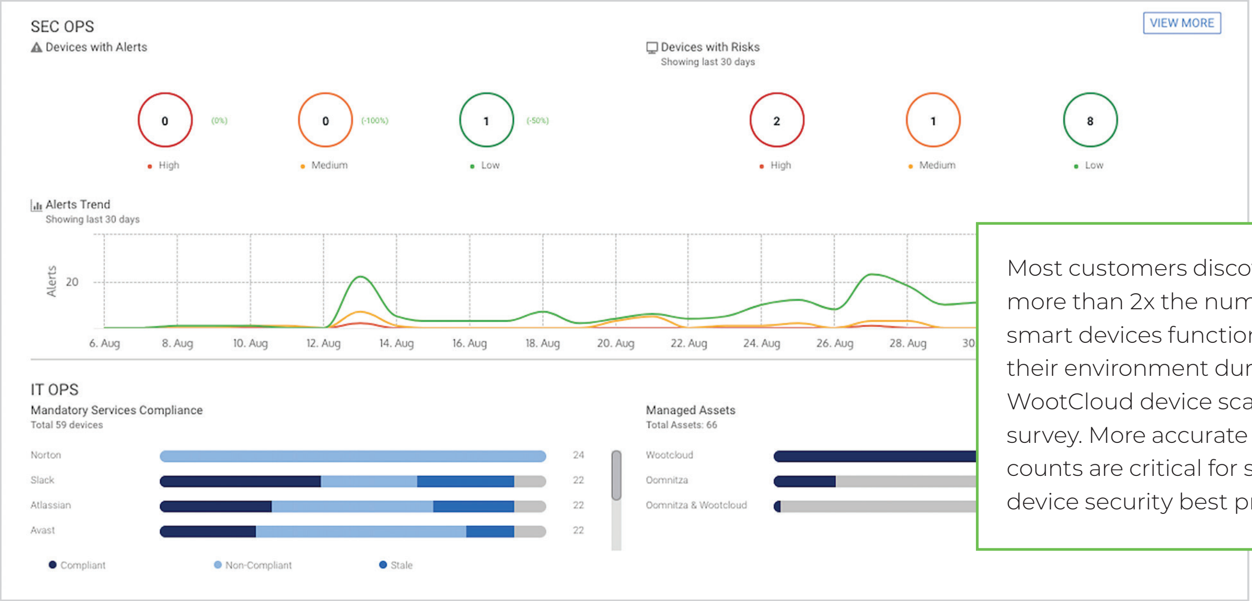
- **Increase in attack surface** — There may never be a way, nor should there be individual IoT device registration by a student or faculty. From fitness apps on watches or jewelry to assistive learning tools, IT teams need to accept that IoT is here to stay in explosive numbers.
- **Sideways motion from smart devices** — Bluetooth-enabled devices which are susceptible to BlueBorne[1] can be used as a gateway to other devices on other radio frequency (RF) spectrums. Bluetooth-enabled devices may likely have a WIFI radio and possibly a network interface card. Those can be used to start a denial of service attack on DHCP servers, or via robotic access points. If there are enough devices affected, it can become a DDoS attack and take down a network.
- **Student Device Vulnerabilities** — From laptops, smartphones, to tablets, printers and watches — these devices are on campuses to stay. Access control policies and device fingerprinting is key to keeping them safe and available.
- **Patching and Security Updates** — CCTV systems, smart routers, and others have all been used in highly-publicized attacks over the last few years, and these are nigh mandatory security systems for campus safety. However, many IT departments argue with physical security on who owns these devices, especially where patches and firmware updates are concerned.

[1] https://www.geeksforgeeks.org/blueborne-attack/

WootCloud provides real-time visibility and insights into everything connected to the education network so IT, IS, and Facilities have a common baseline to make strategic decisions.

ACCURATE SMART DEVICE DISCOVERY

WootCloud's deep device detection technology yields accurate device counts with a low rate of false positives and renders a dashboard showing high-priority risk items requiring remediation. If a device has multiple network interfaces for sharing information, WootCloud correlates these multiple interfaces as belonging to a single entity, providing an accurate accounting of devices.



Most customers discover more than 2x the number of smart devices functioning in their environment during a WootCloud device scan and survey. More accurate device counts are critical for smart device security best practices.

Sample Executive Dashboard showing risk rankings and assets

WOOTCLOUD HYPERCONTEXT® FOR CAMPUS DEVICES

WootCloud profiles every detected smart device on hundreds of attributes known as WootCloud HyperContext®. The attributes below create a deep contextualized intelligence dataset that informs all decisions on network segmentation and access control.

- Association of all the physical interfaces of the device and spectrum of operation of each interface
- Type, Category of the device and related information
- OS, patches, services and applications running on the device
- Functionality or the "purpose in life" of the device
- Micro location of the device, its mobility patterns and times of visibility
- Ownership information of the device and its control information
- Users on the device
- Behavior based analysis of all the data transmissions across all protocols and spectrums
- Risk and vulnerability information, other information collected by other tools used

WootCloud captures more than just device information – WootCloud HyperContext intelligence is more superior and powerful to create strong, unbreakable access control policies.

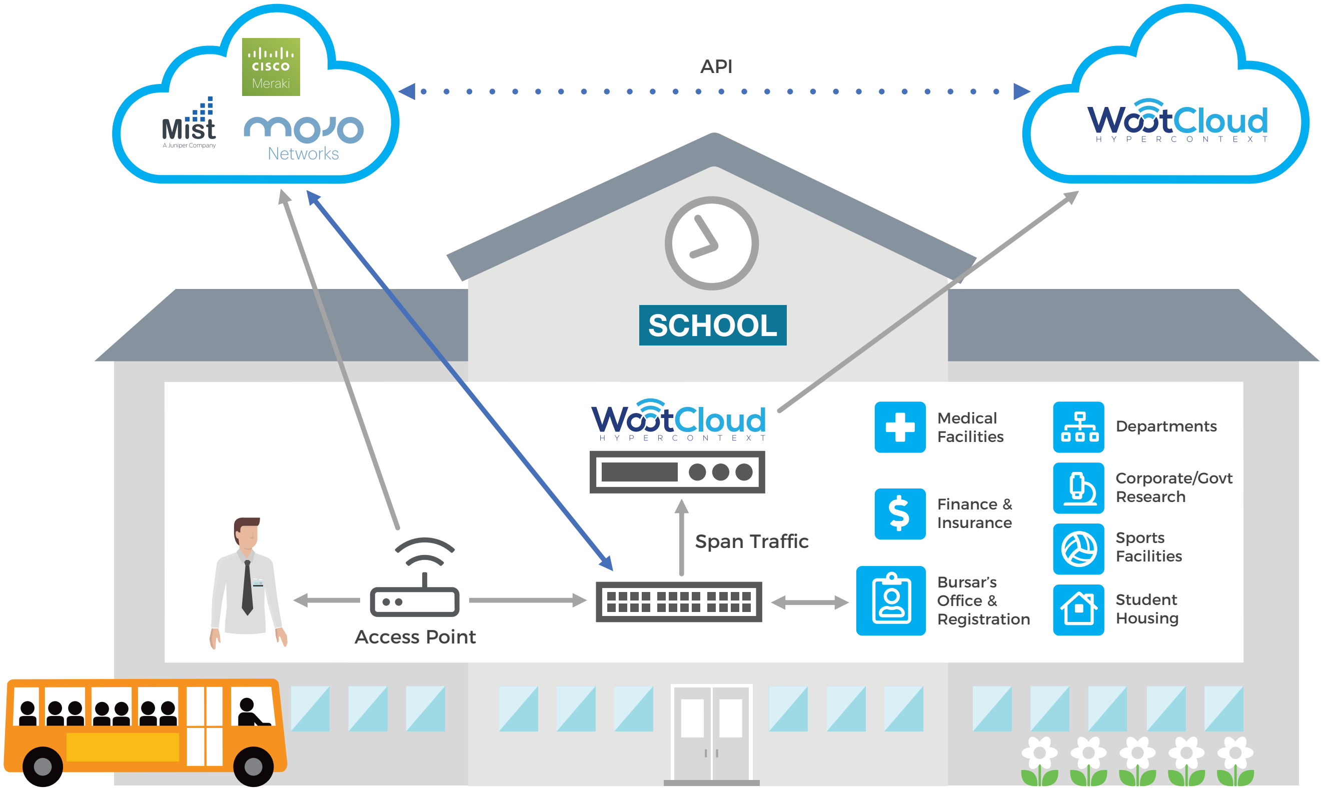
WOOTCLOUD NETWORK SEGMENTATION FOR SMART DEVICES

WootCloud's network segmentation is dramatically simpler to implement, robust and scalable and closes a **glaring gap found in traditional NAC solutions which fail to adequately secure managed and unmanaged devices**. Based on the premise that each device has a completely different risk and threat assessment profile. E.g. a tablet has a different risk profile than a laptop or a workstation — it lets you continuously, dynamically, and automatically segment the network at the device level based on the needs and zones of your educational campus:

By distilling it down to each device, SecOps can

- Auto-enforce granular policies based on device context
- Enable more granular control of network systems
- Better isolate a security flaw if exploited

Physical Properties	Logical Properties	Risk Categories
Device Type	Ownership	Location
Interface	Controls	Time of Operation
Functionality	Department of Use	Bursar's office, Housing, etc.



Providing threat detection relevant to each device type working with OEM partners

Simple rule creation by IT creates "zones" or micro-segmentations of the educational network to protect critical areas

DYNAMIC ACCESS CONTROL FOR SMART DEVICES ON THE MOVE

Smart devices are constantly on the move when needed in different departments, floors and rooms. WootCloud offers NAC-less, software-defined dynamic access control based on security posture, context and real-time threat assessment.

REPORTING FOR RISK MANAGEMENT

WootCloud dashboards are clean, accurate, less noisy (low number of false positives) and rich in context with actionable information providing you centralized device security for all departments.

The Alerts generated provide the Who, Where, What and How information for every smart device, with "actionable next step" guidance. The rich diagnostics & deep investigation capability automates alert handling at scale.

Clear executive briefs for executive-level reporting

WOOTCLOUD'S BUSINESS VALUE FOR UNIVERSITIES, COLLEGES, SCHOOLS

Protecting your students: WootCloud can alert on-campus security, IT Security Operations, etc. in the event of current cyberattacks as well as any new compromised smart device. This secures you a much faster Incident Response and allows for general staff as well as security awareness of potential dangers to daily operation.

Stop many of the major ransomware attacks: Identify many IoT-based system-stopping ransomware in real time. This reduces your potential downtime, not to mention the impact on campus safety.

Automated and dynamic device inventory: Most campuses have never done a full IT survey of every device, let alone specialized smart devices including portable control systems, as part of their network discovery. WootCloud discovers every connected and non-connected device in your environment automatically without requiring a physical search.

Track smart device usage: With a dynamic and exhaustive inventory of all smart and other devices used in each floor and department, you can find lost equipment, use devices more efficiently by calculating peak usage in each department, and potentially reduce over-purchasing of resources which can be reused elsewhere.

DEPLOYMENT

WootCloud can be installed in just a couple of hours using virtual machines, and within a week you can have a complete inventory of devices along with risk scores and suggestions for remediation. Initial remediations are usually done manually, but as more confidence is gained, automated policies can be deployed that will be able to detect and stop attacks of all types, from ransomware to device tampering.

LEARN MORE

www.wootcloud.com

About WootCloud

WootCloud HyperContext® is an agent-less, device focused, network segmentation, access control and threat response platform that automates enterprise security at IoT scale. A privately held company, WootCloud is headquartered in San Jose, California, with offices in India and Argentina.