Data Storage Company Secures Network Access with WootCloud Enterprise Solution

A global data storage company with multiple offices most of which were located in high traffic areas surrounded by restaurants and other retail businesses and large enterprises creating a challenge of multiple unsanctioned access points in the neighborhood. The company had a strong BYOD culture and permitted employees to use their own phones, devices, and peripherals to connect to sanctioned corporate networks. With multiple offices in the same geographic vicinity, employees and vendors constantly changed locations as they traversed these offices for meetings. The company's HR team also needed a scalable way to manage employee separation to ensure that employee devices would not have access to their networks and resources after leaving the company.

Business Challenges

The company wanted to separate out access control both from the perspective of who could access the network as well as which devices were accessing the network. They wanted to use this device visibility and access analytics to also manage employee offboarding from an IP protection perspective. Their challenges centered around:

- Securing Network Control across their multiple offices
- Controlling Network Access for their current and outgoing employees and vendors and their devices

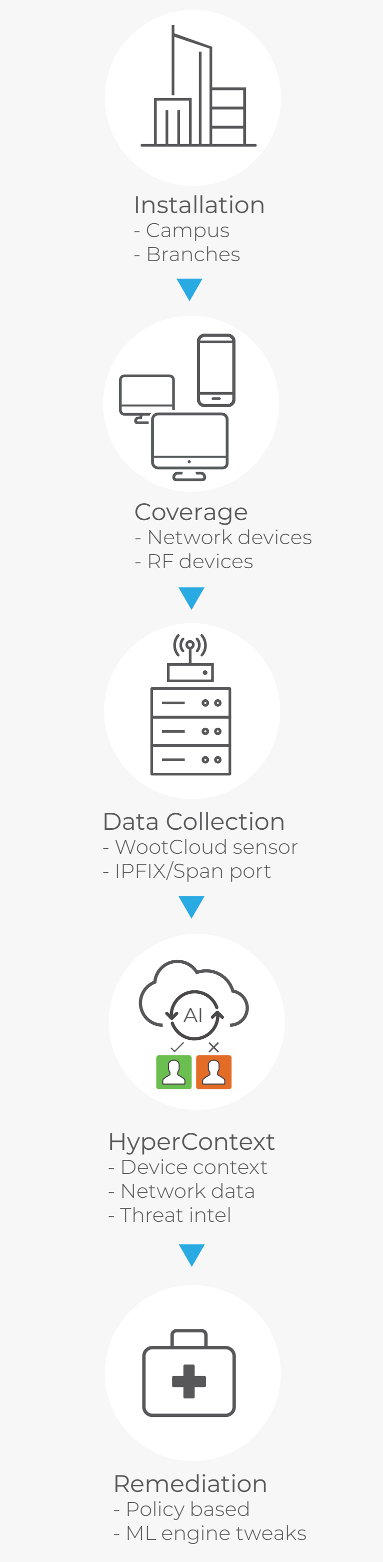
The company needed a solution that would address their device access and control challenges and allow them to control who has access to their network from their global offices, in addition to parsing access across their current employees, outgoing employees, and vendors, and wanted a solution that could be managed from a single pane of glass.

The Solution: Hypercontext Technology

The company selected WootCloud's HyperContext™ technology, using a combination of WootCloud RF and Network sensors to deliver a highly robust, compliance-based access control, restriction, & management solution. This spanned across all of the company's locations and was managed in a single pane of glass. The customer was able to:

- accurately profile and group all the devices entering their network
- segment their network to provide access to sanctioned devices only thus addressing the HR-related issue of cutting off access across all devices belonging to outgoing employees and limiting access to specific segments of the network for external vendors

The WootCloud HyperContext™ Setup



Installation
- Campus
- Branches

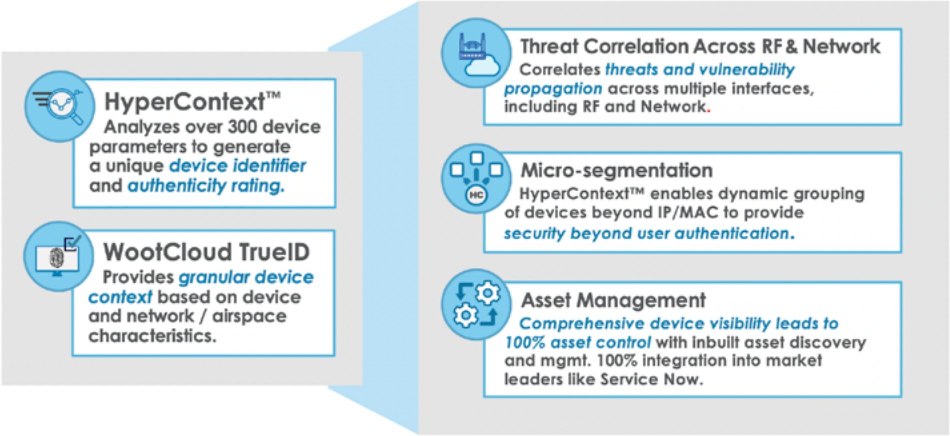
Coverage
- Network devices
- RF devices

Data Collection
- WootCloud sensor
- IPFIX/Span port

HyperContext
- Device context
- Network data
- Threat intel

Remediation
- Policy based
- ML engine tweaks

Unlocking the Full Power of AI/ML Driven Device Security



HyperContext™
Analyzes over 300 device parameters to generate a unique *device identifier* and *authenticity rating.*

WootCloud TrueID
Provides *granular device context* based on device and network / airspace characteristics.

Threat Correlation Across RF & Network
Correlates *threats and vulnerability propagation* across multiple interfaces, including RF and Network.

Micro-segmentation
HyperContext™ enables dynamic grouping of devices beyond IP/MAC to provide *security beyond user authentication.*

Asset Management
Comprehensive device visibility leads to 100% asset control with inbuilt asset discovery and mgmt. 100% integration into market leaders like Service Now.

Business Impact

WootCloud's solution delivered an unprecedented level of command and control over the company's network with preset device access and security policies and profiles that applied automatically when security access credential changes were detected. WootCloud provided preset customer policies and enabled the company to add profiles automatically and in real-time. WootCloud's delivered strict adherence to compliance objectives around network and asset management.

- Employee and vendor compliance with network security policies achieved 100% as measured by pre- and post-implementation surveys with target users.
- Identified unmanaged devices and those not in compliance with MDM requirements utilizing API integrations with MDM and SIEM technologies and network traffic analysis.
- Consistently update devices with policies, integrating it with company's asset tracking and asset management software.

In conclusion, the company was able to know where each item is at any moment of time and was able to control the asset flow in real-time and use real-time information for strategic purposes. In addition, they could ensure better risk management and data security and optimize their operations by ensuring accurate tracing and efficient use of resources and minimizing waste.

For more information, or to contact one of our experts, email here: sales@wootcloud.com or call 1-888-4-WOOTCLOUD.

ABOUT WOOTCLOUD

WootCloud is the only device security platform that uncovers unmanaged devices on both the radio and network spectrum, uses AI/ML to analyze over 300 device parameters to discover gaps in their device and infrastructure risk posture, and the opportunity to close these gaps automatically – all at scale. A privately held company, WootCloud is headquartered in San Jose, California, with industry-leading customers, partnerships with leading security and infrastructure platforms, and top-tier investors.