SOLUTION BRIEF

WootCloud HyperContext® Platform

Context Driven Network Segmentation for Secure Access Controls

What if you could protect every device, every user, every application on your network effortlessly? That's the power of WootCloud HyperContext® 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.

NEED FOR CONTEXT DRIVEN SECURITY

With the explosion in the number and types of connected devices, developing rich context on devices has become of critical importance to ensure security and enforce the right access control to the network. Currently device fingerprinting technologies boil down to type, category, OS, version, which is woefully inadequate, and not enough to make security decisions. To keep networks secure you need to have a deeper understanding of devices entering/exiting your network. This calls for developing device context across multiple dimensions, combining them with machine learning algorithms to generate models and signatures for each device, called HyperContext. This rich contextual device intelligence creates stronger network segmentation and access control policies because it provides the granular nuance that only HyperContext intelligence can provide.

WOOTCLOUD CONTEXT DRIVEN NETWORK SEGMENTATION

Relying on traditional NACs for creating and enforcing network segmentation offers only a coarse-grained segmentation that is hard to manage and easy to break. WootCloud's approach is to use device context intelligence to dynamically create granular secure zones to segment users, workloads, devices and secure them at the device level. It is aimed at automating network security to be more adaptive, flexible, granular and secure.

Using a software defined approach, micro-segmentation is implemented in a layer that is decoupled from the underlying network hardware and NAC tools. This makes the segmentation easier to deploy and manage, operate at IoT scale in an automated fashion and provide security beyond static rules and authentication mechanisms.

QUANTIFIABLE RESULTS

Reduces Threat Hunting Time	>70%
Improves Remediation Time	3X
Operational Efficiency Gain	>60%
FTE Service Savings	1.4 per site/ per shift

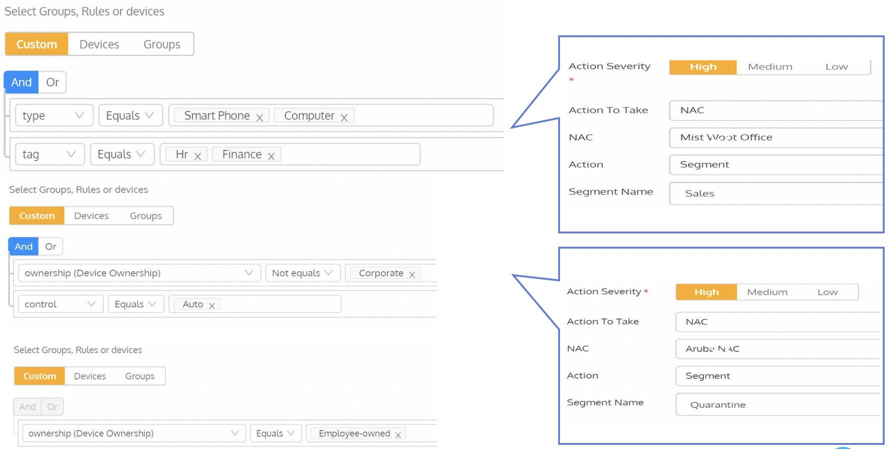
Source: WootCloud Telemetry

PLATFORM CAPABILITIES

- Non-intrusive, AI driven & ML threat detection solution
- Scans devices across multiple spectrums (Network + RF) and dimensions with a deeper capture of device properties and attributes
- Provides rich device context to create deep and accurate policies to manage, track, group, and microsegment devices
- Leverages context driven anomaly detection that leads to lower false positives
- Achieve context driven visibility, asset tracking, compliance, risk and security in a single pane of glass

Operations teams can tailor security settings and create dynamic access control policies that limit network and application flows between workloads based not just on authentication, traffic and application information but by a combination of a device's physical properties, its threat and risk assessment and by dynamic properties like location and time.

Context Based MicroSegmentation



Select Groups, Rules or devices

Custom | Devices | Groups

And | Or

type — Equals — Smart Phone x, Computer x

tag — Equals — Hr x, Finance x

Action Severity *: High | Medium | Low

Action To Take: NAC

NAC: Mist Woot Office

Action: Segment

Segment Name: Sales

Select Groups, Rules or devices

Custom | Devices | Groups

And | Or

ownership (Device Ownership) — Not equals — Corporate x

control — Equals — Auto x

Select Groups, Rules or devices

Custom | Devices | Groups

And | Or

ownership (Device Ownership) — Equals — Employee-owned x

Action Severity *: High | Medium | Low

Action To Take: NAC

NAC: Aruba NAC

Action: Segment

Segment Name: Quarantine

By focusing security and discovery on 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

The more isolated / segmented your network is using device context intelligence, the harder it can be for an attacker to compromise your sensitive systems / data.

Segmentation expertise for every use case

The WootCloud solution addresses a wide array of use cases within Healthcare, Manufacturing and Educational sectors. In every case, the WootCloud platform's flexibility helps to reduce the risk of business disruption and minimize operating costs related to Zero Trust implementation and segmentation projects.

Platform Integrations

WootCloud integrates with Next-Generation Firewalls (NGFW), network access controls (NAC), wireless access points, IT Ops Management, Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) and Configuration Management Database (CMDB) solutions in the market.

Deployment Options

WootCloud supports multiple deployment models including SaaS delivered fully on-premises, private cloud, and MSP hosted.

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.

BENEFITS

Improved Security

Network traffic can be isolated and / or filtered to limit and / or prevent access between network segments.

Better Access Control

Allow users to only access specific network resources from a device centric security point of view.

Improved Monitoring

Provides an opportunity to log events, monitor allowed and denied internal connections, and detect suspicious behavior.

Improved Performance

With fewer hosts per subnet, local traffic is minimized. Broadcast traffic can be isolated to granular subnets.

Better Containment

When a network issue occurs, its effect is limited to a better isolated subnet.

USE CASE

Create policies based on departments, functions, ownership. For example, medical devices owned by the enterprise can only talk to other medical devices owned by the enterprise. Or, finance department assets can only communicate with sanctioned applications and internal resources.

Irrespective of the authentication used, or the network segment that the device is connected to, enforce granular access control based on many different device properties, effectively implementing a zero-trust architecture.

WootCloud
HYPERCONTEXT

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

LEARN MORE

www.wootcloud.com