WootCloud Helps Telco's Defend Themselves and Their Enterprise Clients Against Targeted Device Based Attacks

Telecommunications companies communicate and store vast amounts of sensitive data and their security teams are responsible for managing not only their complex network infrastructure but are also entrusted with the network security of their enterprise clients that depend on them for secure connectivity and guaranteed uptime.

Security teams at telecom providers do everything possible to manage security at scale. In doing so, they are confronted with hundreds of thousands — or even millions — of threat alerts per day which can get overwhelming. WootCloud addresses this precise problem. **We help security teams automatically identify and remediate the highest-risk security breaches across managed and unmanaged devices communicating over the network and in the airspace (Bluetooth, BLE etc.) leading to significant operational efficiencies.**

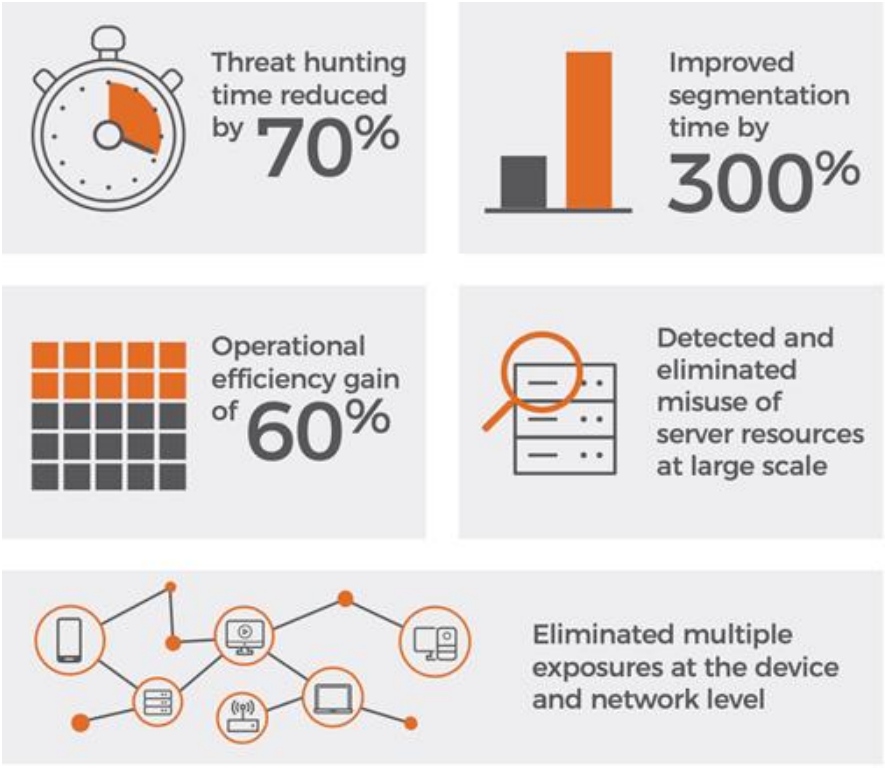

Figure: WootCloud Drives Quantifiable Efficiencies

The devastating impact of bringing down communications and keeping enterprises hostage to ransomware makes the telecommunications industry one of the most targeted industries second only to the healthcare industry. Telecom providers face cyberattacks from two angles:

- Direct attacks from threat groups aiming to breach telecom networks
- Indirect attacks from groups targeting their end-users including enterprise clients of these telecom companies

Some of the most common attack vectors include: Distributed Denial of Service (DDoS) attacks, exploitation of vulnerabilities in the network and consumer devices, phishing or malware and and man-in-the-middle attacks; all due to poor device visibility, lack of adequate device fingerprinting and creating an analytical context of each device as it enters and exits privileged network segments.

According to Ponemon's "2018 Cost of Data Breach Study," telecom providers take on average 173 days to detect a data breach, and 58 days to contain it. In terms of impact, breaches cost telecom providers on average $128 per record compromised and lead to a 2.9% customer churn rate. The cost of an average breach is $ 3.9 M per breach in direct remediation and lost productivity.

The WootCloud HyperContext™ Technology

Our technology can help telecommunication providers in:

1. Identifying Critical Risks in the organization

WootCloud monitors the behavior of every device on and off the network. It is critical to understand what devices are on your network, their intent and interconnections, what access rights are they being granted and what are the policies to allow their access. Monitoring and visibility with WootCloud start with a complete view into every device (network or RF), and a base line of behavioral patterns that can respond automatically to alterations in that behavior. Detecting and observing device interactions within the network to tag anomalies allows WootCloud to vigilantly monitor device behavior and move vulnerable devices away from accessing privileged network segments. WootCloud delivers these processes automatically at machine speed and IoT scale.

- WootCloud consumes vulnerability assessment feeds from existing vendors and also provides its own vulnerability management interface for getting a full picture of vulnerabilities in the environment.
- WootCloud also uses signature matching and advanced ML/AI on traffic to identify emerging threats before they become an issue.
- WootCloud does anomaly detection at an individual device level with a technology called TrueID™ as well as at a device group and operational level.

- We correlate threats from signature and anomalies. Then tie in vulnerability assessment to provide a risk score for every device in the organization.

2. Making Better Decisions

HyperContext technology allows customers to view and group users and devices in categories to understand and predict the behavior of any device over time. It provides an unprecedented level of command and control over the network landscape with context that reduces incident response times over 70% faster than manual solutions. HyperContext helps telecom security leaders make informed decisions about where and how to invest their resources for maximum effect.

WootCloud also enables you to supercharge your existing security solutions such as SIEMs by appending enhanced device insights to the data & feeding it into orchestration workflows. HyperContext's policies can be integrated into the runbooks and playbooks of a SOAR (Security Orchestration, Automation and Response) tool to supercharge the SOC and reduce incident response time. In doing so you get more out of your SIEM and SOAR investments by:

- Enriching alerts with deep WootCloud HyperContext. This provides all the information on the device needed along with the incident which enables the operator to quickly handle threats, reducing incident response times.
- Generating alerts on RF and Network Anomalies. WootCloud's HyperContext correlated anomalies surface true threats and thereby reducing alert fatigue.
- Measuring and Managing Assets and Compliance — by automating them through SOAR Runbooks. This improves IT security hygiene and helps in incident prevention.
- Block & Quarantine through SIEM policies or SOAR Runbooks.

3. Moving Beyond Reactive Security

Along with identifying threats, WootCloud is a preventative solution. WootCloud creates visibility to all devices and is unique in its ability to encompass device based micro-segmentation based on custom grouping of devices by corporate functions (Finance department devices or point of sale systems) to compliance posture (devices get segmented based on whether they have an MDM client like Airwatch on them) or acceptable risk (based on our risk qualification engine). WootCloud works with access point vendors like Juniper's Mist Systems to eliminate current Network Access Controllers and get the next level of access restriction and access control. These actions are done dynamically, and automatically. WootCloud allows access privileges to fluctuate based on user behavior and their privileges. All of WootCloud's labels and context can be used for

- Context & device behavior driven policy management
- Nuanced access restrictions and controls for every device based on contextual information all the way from micro-location to ownership to traffic patterns.

HOW IT WORKS

ARCHITECTURE CLOUD

Additional Resources:

- WootCloud overview video - https://wootcloud.com/#
- White paper- Securing Smart Devices
- White paper - CISOs Guide to Improving Security Risk Posture
- Solution brief - WootCloud Solution Brief
- Schedule a demo
- Enjoy a complimentary smart device assessment for your organization