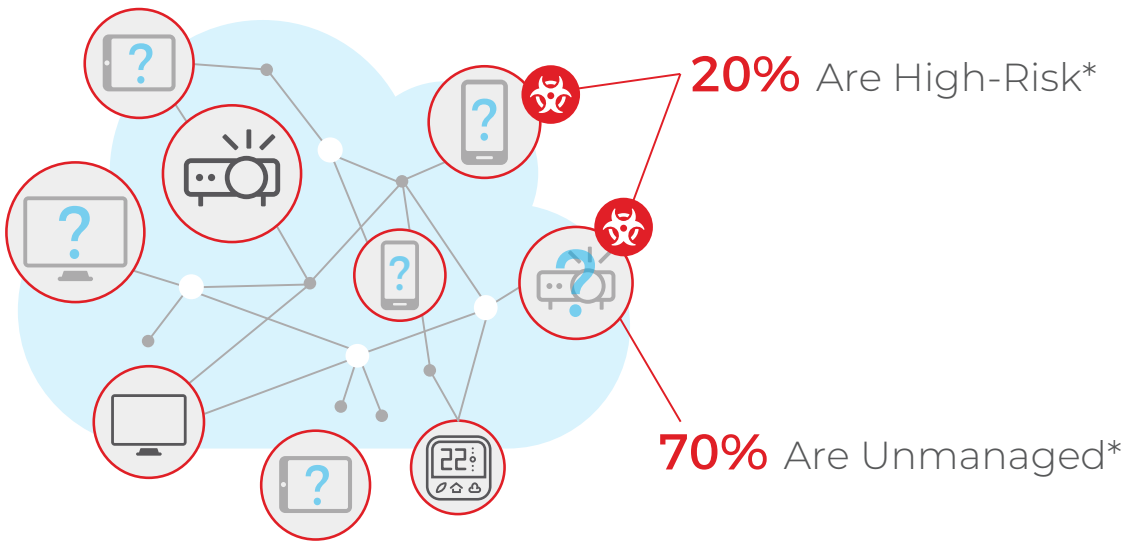
Contextualized Visibility and Control to Secure Smart Devices

WootCloud's HyperContext™ Transforms Smart Business Device Security

INTRODUCTION

The rapid proliferation of interconnected business-oriented smart devices has exponentially expanded every organizations' attack surface, increasing the likelihood of cyber-attacks that place homes, businesses, healthcare providers, governments and defense organizations at risk of data loss and network breaches. Most enterprises and governments are already under constant and unyielding attacks by rogue nation states and cyber criminals, yet they typically overlook smart devices as a significant attack vector for such attacks, despite the fact that recent high profile device breaches in the news only scratch the surface of the magnitude of the problem that exists today. Our analysis shows that for every incident detected, there are at least three that go unrecognized or unreported. Existing endpoint security, network security, cloud security, and data loss prevention (DLP) solutions may work well to protect traditional IT infrastructure. However, they are completely outclassed and outmaneuvered by the new security challenges posed by interconnected smart business devices as varied as IP-based cameras, smart TVs, set top boxes, and smart thermostats.

Increasingly, the requirement for organizations to connect, communicate with, and remotely manage a staggering number of networked smart devices via the Internet is the new normal. And this transition from closed networks to public internet is occurring from the factory floor to the connected enterprise, from the oil and natural gas industry to warehouses and homes. Gartner Research, in fact, lists security for these devices as the #1 challenge to making the Internet of Everything a reality.



Explosive Smart Device Growth	$1.7 trillion market (IDG Forecast) By 2020	50 billion devices (Forbes) by 2020	$117 billion market in Health Care alone
New Security Challenges	– 70% of devices have vulnerabilities – Unpatched	– 80% use default usernames and passwords – Easy to exploit	90% store personal and credentials in the clear

The most common challenges to securing interconnected smart business devices include:

- Smart device manufacturers have very little background in dealing with security, and there are no security standards driving trusted software development on these devices.
- In most cases, smart devices have limited computing power, memory, and bandwidth and thus cannot have a security solution installed.
- Many smart devices store and send sensitive data, including credentials, in plain text.
- Default smart device configurations and passwords are public information. In many cases, customers deploying these devices continue to use the default credentials.
- Devices are interconnected over LAN, WAN and PAN. A single attack can affect the entire network of connected devices.
- Due to the complex layers of smart device systems, it's hard to identify where any one problem is originating from.
- Smart devices occupy multiple communication spectrums like WiFi, Bluetooth, BLE, and ZigBee.

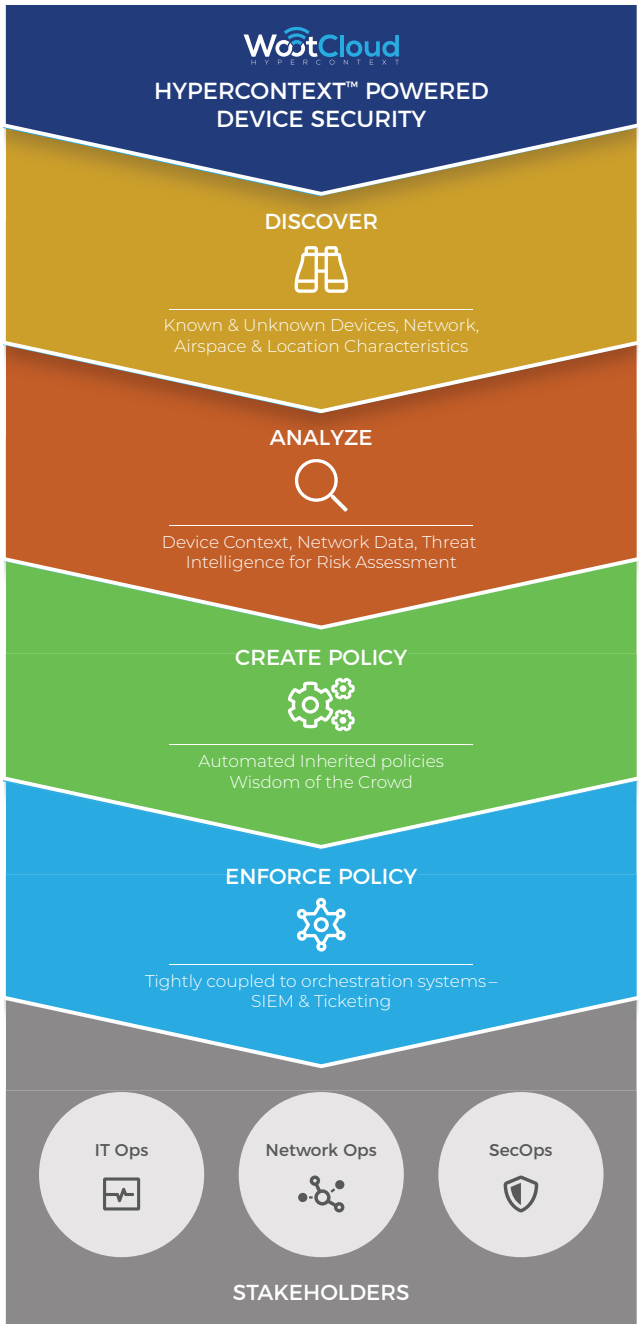
In view of this digital device explosion, corporations the world over are struggling to find answers to the following questions:

- How do we protect billions of these devices and the network they communicate on from intrusions, attacks, and interference that can compromise personal privacy and threaten public safety?
- How do we manage this risk and conduct business in a safe and secure fashion?
- How do we protect critical devices and systems from attacks?

The only way to address these challenges is through a holistic and robust security approach that covers the full lifecycle of the device and its communications. Current solutions take a piecemeal approach to device security, with some vendors focusing on hardware, some on encryption, and some on device certifications. These approaches, even in combination, still leave major vectors vulnerable to attack.

WOOTCLOUD HYPERCONTEXT: BUILT FROM THE GROUND-UP TO SECURE SMART BUSINESS DEVICES

The WootCloud HyperContext Platform is built to provide actionable insights by combining device context, network data and threat intelligence from many traditional and non-traditional sources of collection. It enables companies to understand risks from unmanaged, transient devices and enforce a unified policy across all their campuses. WootCloud is the industry's only full spectrum visibility and analytics platform that tightly integrates with existing security solutions to simplify and strengthen the security posture of organizations by minimizing the attack surface presented by smart devices.



In addition to securing the devices themselves, WootCloud helps build an awareness among IT and operations administrators of risk and risky behavior in their smart device networks. This is achieved via a multi-layered approach to security that involves four components: **Discover**, **Analyze**, **Create Policy**, and **Enforce Policy**.

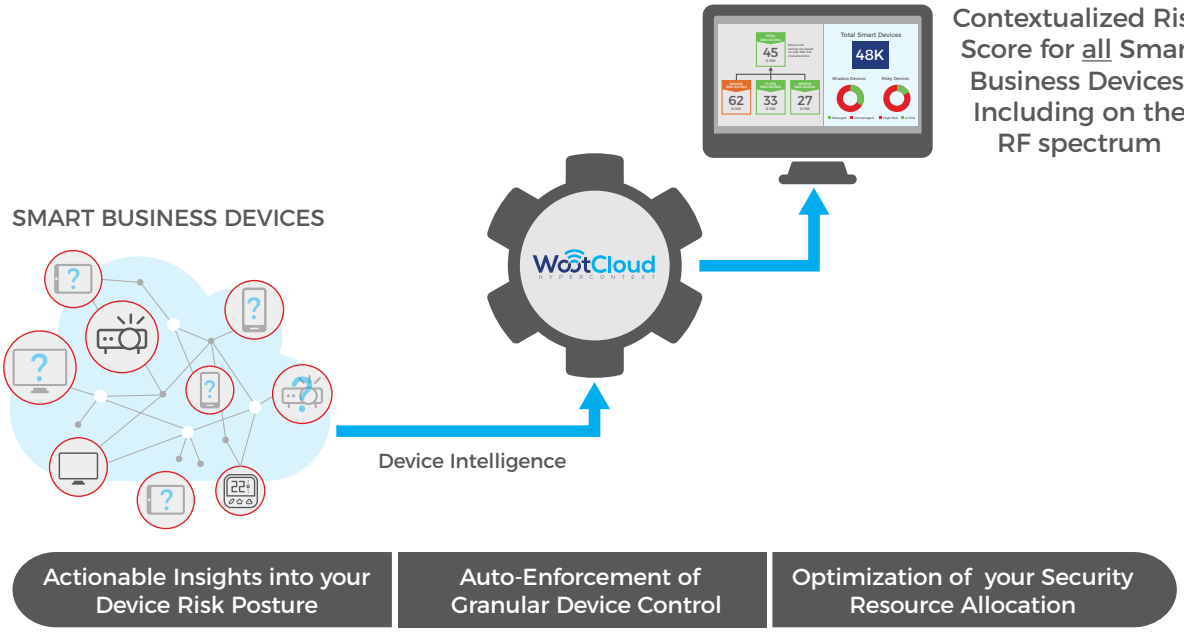
DISCOVER

According to the Hiscox Cyber Readiness Report 2019, a staggering 74% of WW companies surveyed failed to meet the threshold of cyber-readiness. Firms are less confident in the efficacy of the security measures they have put in place, and in many areas, confidence has been declining ever since the first reported findings in 2017. Furthermore, many systems used for audit process only account for the company managed devices, but do not list unmanaged devices like personal devices, audio-video components, telecommunication devices, smart wearables, etc. brought into the company. This is especially important in the current work environment where unmanaged devices far outnumber the devices that the enterprise owns and manages.

WOOTCLOUD HYPERCONTEXT

- Provides unparalleled visibility into the connected device infrastructure to reveal existing vulnerabilities and threats.
- Provides a view across multiple communication spectrums and ties these spectrums to a single device.
- Presents organizations with device information which includes state information from physical, logical, operational and locational touch points. Information like their interfaces, ownership, control, functionality, access rights, risk assessments, operating systems, images, patches and configurations amongst others.

WootCloud HyperContext uses a proprietary algorithm to calculate a unique risk profile for each device. This unparalleled, near real time, multi-site visibility into devices provides deep insights to the security team both to prevent and triage attacks.



ANALYZE

WootCloud monitors all devices, their connections, their data and the network across multiple communication spectrums. It also monitors peer to peer over the air communications such as WiFi, Bluetooth, BLE, and Zigbee. It inspects traffic, logs and correlates data, performs deep packet analysis and content inspection to provide a very fine-grained analysis of every device in the organization from individual devices to device groups and organization wide operational identity and context. WootCloud's industry-specific protocol filtering and deep packet inspection capabilities are useful to identify malicious payloads hiding in these custom protocols and communication spectrums.

WootCloud's device identity fingerprints accurately recognize each individual device, group devices of the same kind, and establish the device's normal operation and function. This deep context is then used to:

1. Identify and fingerprint all new devices seen in the organization automatically
2. Identify all anomalous behavior at device level
3. Offer insights and analytics about the device level risks, threats associated and best practices around mitigating such threat profiles
4. Generate labels based on all the collected information, intermediate insights and final fingerprints and expose these labels to WootCloud's proprietary industry-leading policy engine

WootCloud's industry-specific protocol filtering and deep packet inspection capabilities are useful to identify malicious payloads hiding in these custom protocols and communication spectrums.

POLICY ENFORCEMENT

The security policy created in the HyperContext platform and processed in WootCloud's powerful policy engine offers a nuanced remediation and control stance that denies infected devices the opportunity to spread their malware any further. Security and access rights cannot be static, especially when the number of devices accessing the network is ever increasing As devices enter and leave a network, dynamically controlling the access these devices and users have to other resources in the network based on context and real time threat assessment is paramount. Static rules based on L2-L3 based segmentation, ACLs and user authentications are draconic and can be easily circumvented. For example, if the audio video conferencing devices are statically segmented into a specific subnet, it is easy to plug in a laptop in the same subnet and snoop on the SIP communications. It is also easy to make a mistake and plug in a conferencing device into other subnets. A dynamic approach would entail a learning engine and a policy engine that determines a device as a video conferencing device and automatically routes it to correct VLAN with the proper access permissions. On the flip side any device on the subnet that does not match the profile of a conferencing device or displays anomalous behavior can be quarantined from other devices in that VLAN.

Devices and users are now mobile and Zero Trust Architecture should also be able to adapt not just to different locations but also micro locations(floor/bay/workstation) within a specific location. With WootCloud, it is now possible to dynamically associate the right security and access permissions to devices as they move between floors, buildings, cities or countries.

The time has come that the perimeter, access control and quarantining of devices is software defined and dynamic. Device security postures should be continuously monitored and adapt to the current state of the device, network, threat exposure and should not be defined as static rules.

WOOTCLOUD: CONTEXTUALIZED VISIBILITY & CONTROL FOR SMART DEVICES

Securing smart devices and the network they operate in is critical to prevent successful cyber-attacks. The solution needs to intelligently recognize and counteract threats. According to the Ponemon 2019 Cost of a Data Breach Report, there is an estimated 28 billion devices expected to connect to networks in the next couple of years — and that the cost of a global data breach in 2019 is approximately $3.9 million — organizations cannot afford to have any hidden devices in their business environment going unnoticed and unprotected.

The WootCloud HyperContext solution is the only enterprise device security solution that successfully leverages both the radio and network characteristics to neutralize device threats and empowers security and IT teams to identify both managed and unmanaged devices and proactively control access. The company's scalable, agentless deployment capabilities, covering 100 percent of a network, enables actionable insights to detect behavioral anomalies faster at a lower cost.

The time is now for both C-level and IT managers to ask themselves if all the devices in their environment are truly secure and, if not, how they can change their strategy to protect it effectively.

NEXT STEPS

Request a WootCloud HyperContext demo

Request a free WootCloud Smart Device Risk Assessment

About WootCloud

WootCloud is the only enterprise device security solution provider to leverage both the radio and network characteristics to neutralize device threats. WootCloud's unique HyperContext™ platform empowers security and IT teams to identify both managed and unmanaged devices and proactively control access. The company's scalable, agentless deployment capabilities, covering 100 percent of a network, enables actionable insights to detect behavioral anomalies faster at a lower cost.

WootCloud was one of the select companies to win the prestigious 2017 Tie Silicon Valley Top 50 Startups Award. A privately held company, WootCloud is headquartered in San Jose, California, with offices in India and Argentina.

WootCloud HYPERCONTEXT

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