WootCloud
HYPERCONTEXT

6 Steps to Securing Devices at IoT Scale

A Proposed Guide to Truth, Trust and IoT Device Security

TABLE OF CONTENTS

TRUST BUT VERIFY has been one of the primary principles of IT security for many years. With traditional perimeter-based and endpoint security, enterprises followed the trust but verify path through a number of proven practices:

- Protect the ingress and egress from the network
- Define and group devices and users into subnets/VLANs using a specific set of usually static rules
- Use authentication mechanisms centered around users
- Install agents to detect and prevent malware

But today, these methods, though still necessary, are no longer enough to protect against the threats posed by unmanaged devices, credential misuse, IoT devices, wrong configuration, insider mal-intent, and lateral movement of threats, once they enter the system.

Moreover, while existing endpoint security, network security, cloud security, and data loss prevention (DLP) solutions may work well to protect traditional IT infrastructure, they are completely outclassed and outmaneuvered by new security challenges — more specifically, the security challenges posed by smart business devices such as IP-based cameras, smart TVs, set top boxes, and smart thermostats.

The problem of IoT devices using default passwords is perhaps the biggest and best-known vulnerability. Yet in a similar way, devices that aren't actively managed can also become vulnerable over time, and networks also present serious security issues.

Spurred by concerns such as these, the Zero Trust approach to security is gaining strong momentum. Rooted in the principle of "always verify, never trust," the approach is designed to address security, access privileges and control in the network by leveraging micro-segmentation and performing granular access enforcement based on users, devices, data and location properties. Implementing an effective micro-segmentation strategy along these principles will require the orchestration of a number of established and emerging technologies into a cohesive whole. We propose the following six steps as a road map toward realizing these objectives.

While existing endpoint security, network security, cloud security, and data loss prevention (DLP) solutions may work well to protect traditional IT infrastructure, they are completely outclassed and outmaneuvered by new security challenges

1

PLANNING FOR ALWAYS VERIFY, NEVER TRUST ARCHITECTURE

Coping with Untrusted Devices

Increasingly, the “new normal” for many organizations involves connecting with and remotely managing a staggering number of networked smart devices via the open Internet. This transition from closed networks to public internet is occurring across all kinds of organizations and industries, from healthcare and retail, to the factory floor to warehouses and homes. Unfortunately, effective security for connected devices hasn’t kept pace, and many organizations continue to overlook smart devices as a significant attack vector for cyberattacks. Gartner, in fact, lists security for smart devices as the #1 challenge to making the Internet of Everything a reality.

Gathering Intelligence on Your IoT Environment

Each user, device, data flow, and location should be monitored and observed continuously, even those which have authenticated correctly — because as we all know, credentials can be stolen. Monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Doing this successfully will require deep context about every device, resource and user in and around the network and the ability to:

- Dynamically micro segment these devices based on context and geo location.
- Control user access to these devices based on context and real-time threat assessment.
- Automatically handle devices at IoT scale via a policy-driven engine.

Each user, device, data flow, and location should be monitored and observed continuously, even those which have authenticated correctly

2

DISCOVER AND EVALUATE ALL MANAGED AND UNMANAGED DEVICES CURRENTLY ON YOUR NETWORK

Many systems used for audit process only account for company managed devices, but do not list **unmanaged** devices such as personal devices, audio-video components, telecommunication devices, smart wearables, etc. This shortcoming is becoming increasingly important in the current work environments where BYOD (bring your own device), choose your own device (CYOD), and COPE (corporate-owned, personally-enabled) have become commonplace policies. In fact, it's now the case within many organizations that unmanaged devices far outnumber the devices that the enterprise owns and manages, and it's expected that IoT devices will soon outnumber BYOD and other mobile devices in the enterprise.[1] As such, a discovery capability for all existing devices currently on your network is essential.

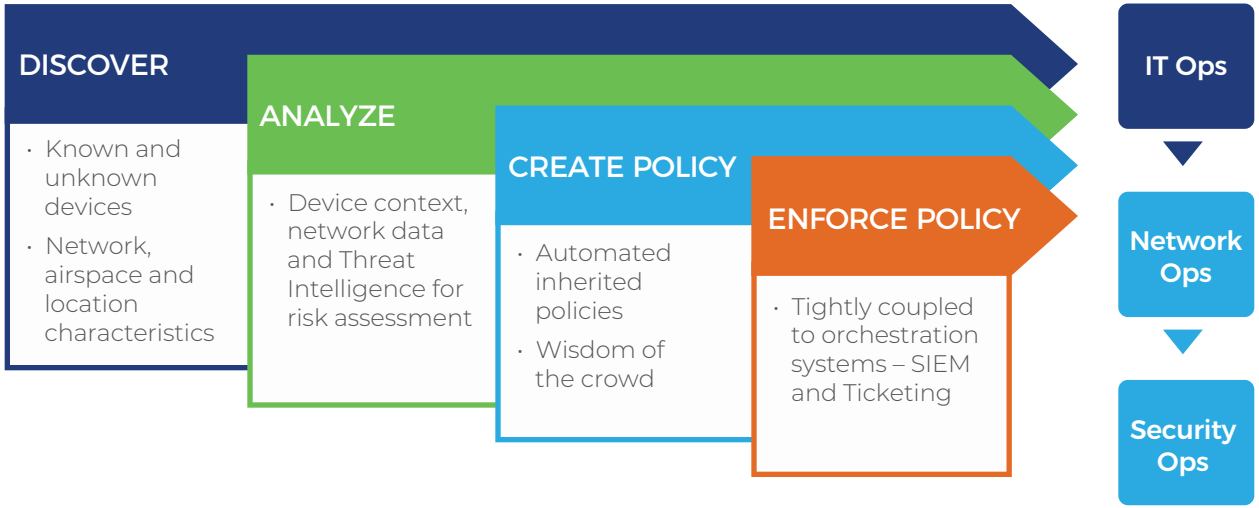
Automated discovery of new devices is an essential capability as well. With an explosion in the number of electronic devices that are now connected via multiple communication protocols, fingerprinting the device needs to be done based on the unique characteristics of the device across multiple dimensions. The dimensions needing to be measured include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. Ideally, you want to have the capability to generate a model or signature for each device based on the following parameters:

- Association of all the physical interfaces of the device and the spectrum of operation of each interface.
- Type and 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 of 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.

IoT devices will soon outnumber BYOD and other mobile devices in the enterprise.

[1] Ericsson Mobility Report, Rima Qureshi, Sept. 2016

WOOTCLOUD HYPERCONTEXT™ POWERED DEVICE SECURITY



All the collected data and the intermediate insights are then used to develop a device identity fingerprint, device group fingerprints, and device operational fingerprints. These fingerprints accurately recognize the device, group devices of the same kind together, and establish the device's normal operation and function. This can then be used to establish an effective architecture by:

- Automatically identifying new devices seen in the organization.
- Uncovering anomalous behavior in the devices whose fingerprints have been collected.
- Providing insight into risks and threats to inform best practices over time.
- Generating labels based on all the collected information, intermediate insights and final fingerprints, and expose these labels to the micro-segmentation and policy layers.

3

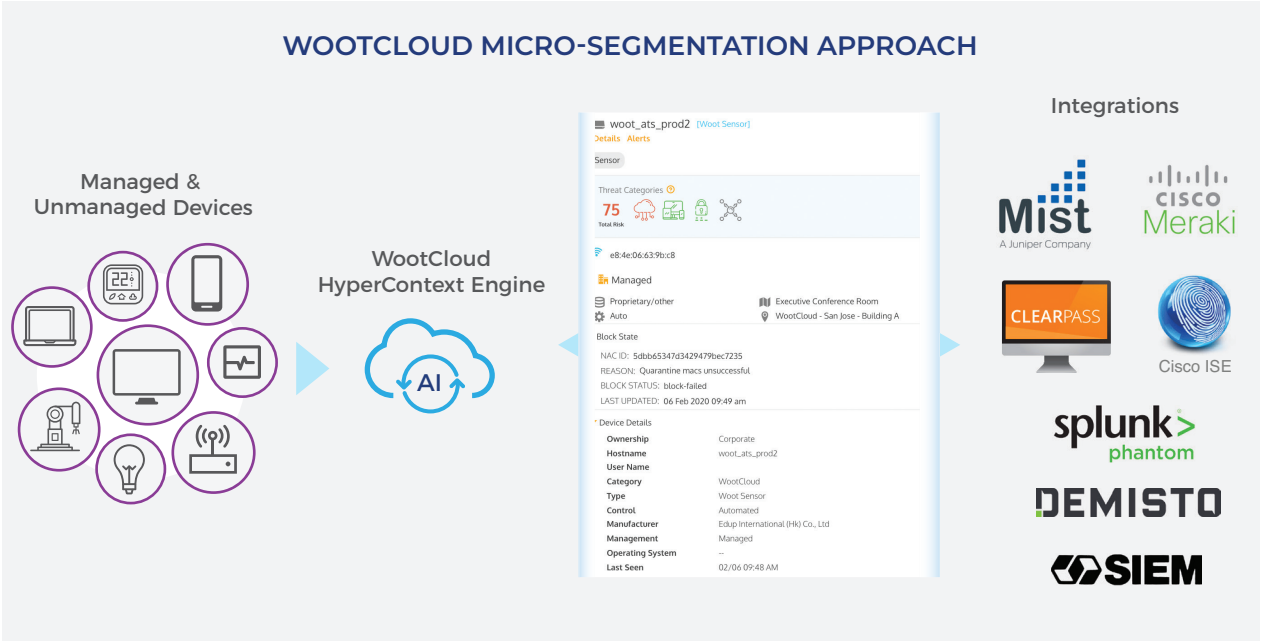
WHY THE NEED FOR MICRO-SEGMENTATION

Network segmentation has long been accomplished by network access controls (NACs) including segmentation firewalls, VLANs, authentication, and access control lists (ACLs). These first- and second-gen network security control points offer coarse-grained segmentation that can be expensive and hard to manage, and represent no surety for a compromised device.

Micro-segmentation, alternatively, is a much more granular and dynamic control methodology to create secure zones in and around your network, between your network, and any cloud services you may use.

Instead of a single gating permission like IP combined with one authenticated credential, micro-segmentation utilizes the deep context of devices, and affords automation to isolate workloads, devices, and even users from one another.

This layer of segmentation is a software implementation — a software-defined access control layer decoupled from the traditional hardware and NAC tools. Logical software segmentation is easy to deploy and manage, and scales with your IoT adoption automatically to provide security beyond static rules and authentication mechanisms.



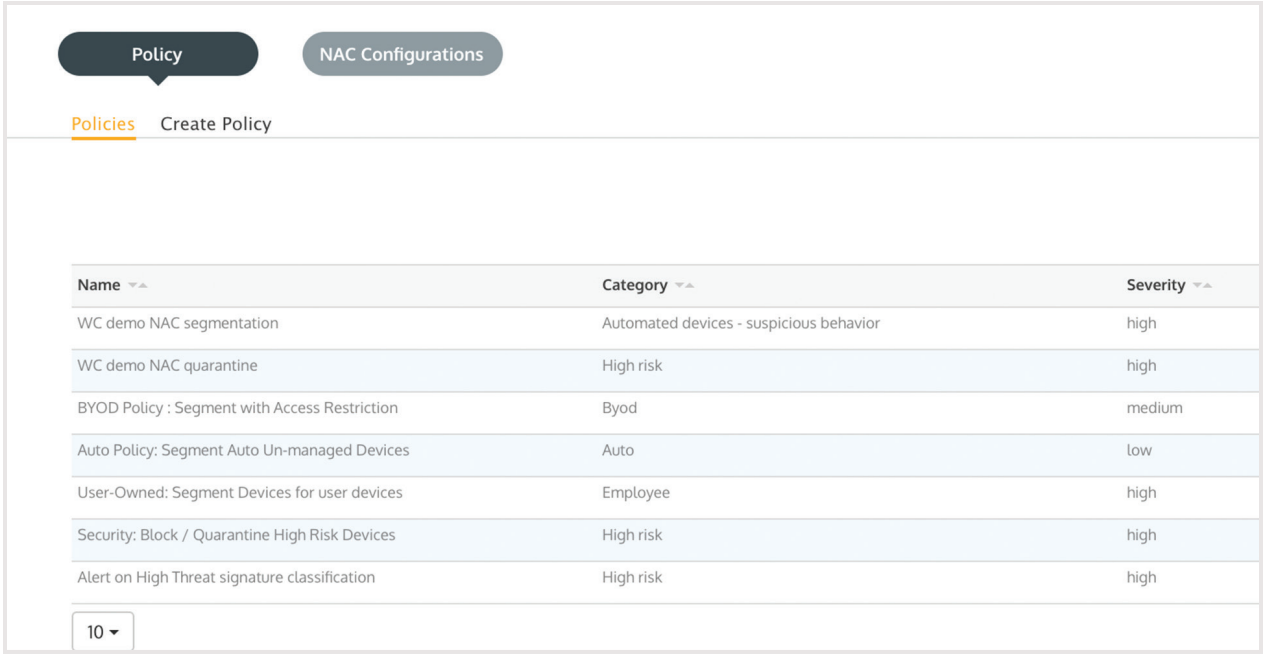
Instead of a single gating permission like IP combined with one authenticated credential, micro-segmentation utilizes the deep context of devices, and affords automation to isolate workloads, devices, and even users from one another.

4

CREATE POLICIES FOR DEALING WITH UNSANCTIONED IOT CHANGES

With strong device context, micro-segmentation becomes a reality. Network operations teams can now 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 physical properties. These would include factors like device type, interface and functionality; logical properties such as ownership and control; by threat and risk assessment; and by dynamic properties like location and time.

In this security model, a company could set up a policy, for example, that states that medical devices owned by the enterprise can only talk to other medical devices owned by the enterprise or a policy that finance department assets can only communicate to sanctioned applications and sanctioned internal resources. Thus, regardless of the authentication used, or the network segment that the device is connected to, it becomes possible to enforce a far more granular access control based on many different device properties. And if a device or workload moves to a different location, the security policies and attributes move with it.



Regardless of the authentication used, or the network segment that the device is connected to, it becomes possible to enforce a far more granular access control based on many different device properties

5

INTEGRATE DEEP DEVICE SECURITY WITH MONITORING AND RESPONSE TOOLS

With all the device labels and fingerprints generated, processes like access control, vulnerability scanning, and risk escalations can all be automated via policies. You can then ensure that the flow of events into your security monitoring and event management systems, and thus into your Security Ops team, are rigorously vetted and kept only to serious incidents requiring response. Integrating deep device security with intelligence into existing security practices and processes will require that perimeter, access control and device quarantine capabilities must be 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.

Monitoring and Dynamic Controls

The architecture should be able to adapt not just to different locations but also micro-locations within a given building group environment. In practice on a corporate campus or similar physical environment, this would function along the following lines:

- As a device moves between floors or between buildings, it would be provided with the right security and access permissions.
- Automated, policy-driven monitoring ensures that devices have the right configurations, meet the right compliance goals, and have the correct access they need.
- Only anomalous devices not responding or repeatedly failing the automated policy controls would then be surfaced to the operations team; in this way, workload is reduced.

Device security automation aids in a low-friction deployment of a verifiable architecture by:

- Better use of security operations team assets, improving ROI on existing security tools and technologies.
- Quicker response to incidents and events.
- Increased productivity by reducing security operations fatigue.

Integrating deep device security with intelligence into existing security practices and processes will require that perimeter, access control and device quarantine capabilities must be software defined and dynamic.

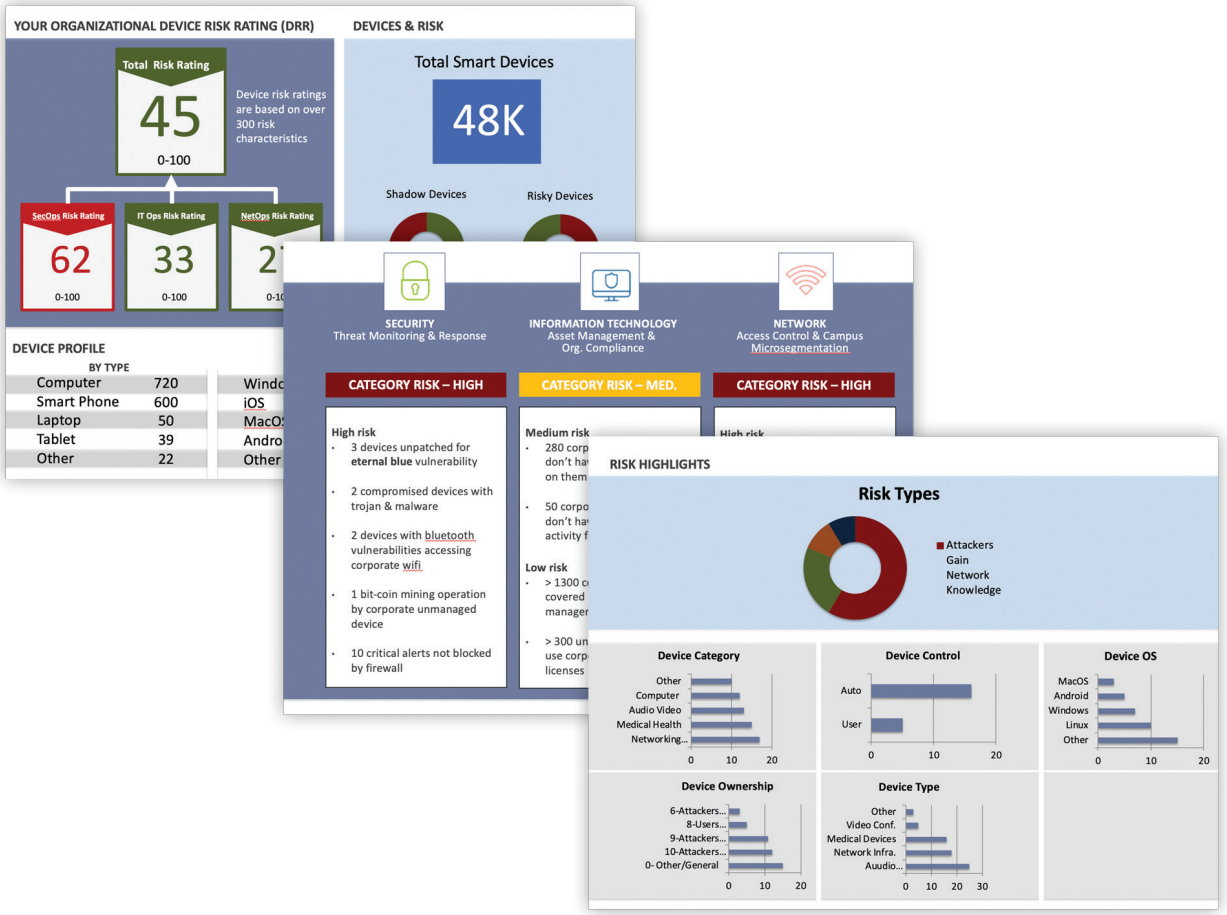
The architecture should be able to adapt not just to different locations but also micro-locations within a given building group environment.

Measure and Communicate Risk Posture

Micro-segmentation can help improve your regulatory compliance posture by completely isolating systems that are subject to regulations from the broader IT infrastructure.

Micro-segmentation can also tightly govern how systems within regulatory scope communicate with each other, reducing the risk of non-compliant usage.

The added visibility that micro-segmentation provides can also accelerate and improve the audit process.



6

INCIDENT RESPONSE AND INVESTIGATION

Securing smart devices and the network they operate in is critical to prevent damaging cyber-attacks. Most enterprises and governments are under constant and unyielding attacks by rogue nation states and cyber criminals, yet many 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.

As such, your device context profile and micro-segmentation approach needs to intelligently recognize and counteract threats. What's needed is an enterprise device security solution that:

- successfully leverages both the radio and network characteristics to neutralize device threats.
- provides actionable insights by combining device context, network data and threat intelligence from many traditional and non-traditional sources of collection.
- enables companies to understand risks from unmanaged, transient devices and enforce a unified policy across all their campuses.
- empower security and IT teams to identify both managed and unmanaged devices, and proactively control access.

In addition to securing the devices themselves, this type of solution helps build awareness among IT and operations administrators of risky behavior in their smart device networks.

What's needed is an enterprise device security solution that successfully leverages both the radio and network characteristics to neutralize device threats.

CONCLUSION

TOWARD A TRUTH, TRUST AND IOT DEVICE SECURITY ENVIRONMENT

By integrating deep device context with micro-segmentation you can:

- **Reduce your overall attack surface** by preventing lateral movement of malware and threats.
- **Improve breach containment**. Without a structured micro-segmentation approach in place, tactics such as probing for vulnerabilities, installing malware, and establishing unauthorized communication backchannels will have a much higher success rate.
- **Provide stronger regulatory compliance posture**. Micro-segmentation can completely isolate systems that are subject to regulations from the broader IT infrastructure. Micro-segmentation can also tightly govern how systems within regulatory scope communicate with each other, reducing the risk of non-compliant usage.

See WootCloud HyperContext™ in Action

Click on this link to schedule a demo. You can also enjoy a complimentary smart device assessment for your organization.

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

About WootCloud
WootCloud is the only smart device security platform that uncovers unmanaged devices on both the radio and network spectrum, and analyzes over 300 device parameters to generate device risk scores. This helps organizations discover gaps in their device risk posture and the opportunity to close these gaps. A privately held company, WootCloud is headquartered in San Jose, California, with offices in India and Argentina.

WootCloud
HYPERCONTEXT

For more information, visit us online at **www.wootcloud.com**