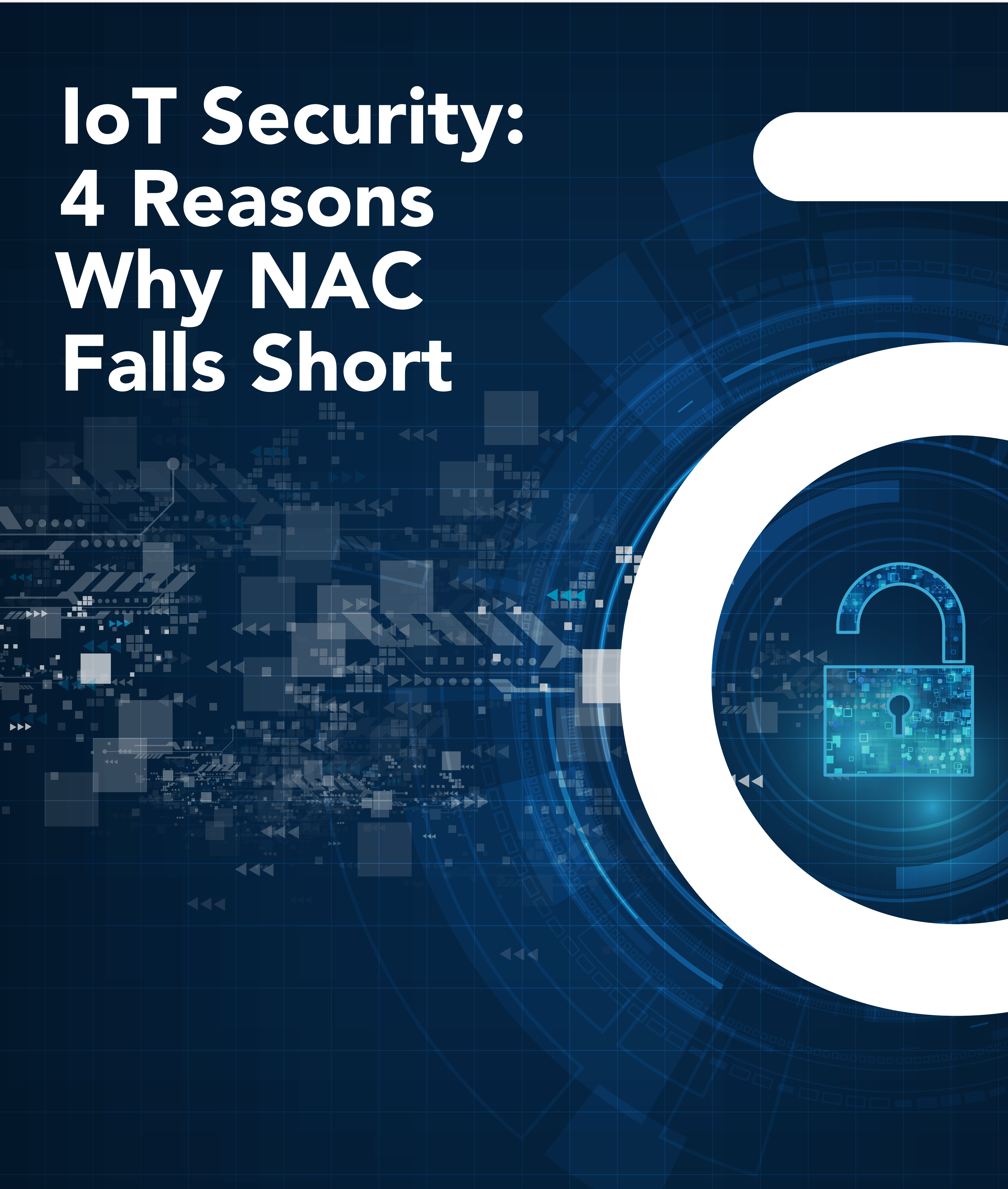
WHITE PAPER

4 REASONS WHY NAC FALLS SHORT

ordr

IoT Security: 4 Reasons Why NAC Falls Short



Worried about the growth of unmanaged and IoT devices?

According to International Data Corporation (IDC), there will be 41.6 billion connected IoT devices, or "things," in 2025 – all of which need to be secured. When it comes to access control, and the ability to allow or deny access, most networking and security teams automatically think of NAC solutions. But, is NAC the right solution to secure IoT?

There are several core use cases that are often associated with NAC – performing user authentication, checking that laptops and workstations meet company policy, and managing access for wireless devices.

However, if the focus is to is **gain visibilty and control over unmanaged devices including IoT and OT** – identifying all unmanaged assets, preventing rogue devices, segmenting vulnerable devices – there are more efficient approaches available.

In this paper, we provide 4 reasons why NAC may not be the right fit if your specific objective is to secure unmanaged and IoT devices. We present an alternate solution using the Ordr Systems Control Engine.

(**Note:** If you've already deployed NAC, and want to accelerate your deployments for unmanaged and IoT devices, check out our other guide "**Accelerating NAC Deployments for IoT**".)

1 NAC Has Poor Visibility of IoT Devices

The rise of IoT and OT devices are often cited as one of the drivers behind the adoption of NAC. However, in most cases these and other unmanaged devices are uniquely challenging to control with NAC. These challenges often stem from a fundamental lack of visibility into IoT devices themselves. NAC typically lacks the ability to identify the type of device in question (e.g. security camera, HVAC system, CT machine, etc), as well as details that will be important for making management and access decisions such as its make, model, and other details. With this lack of detailed visibility into Iot devices, it is very difficult for organizations to track which assets are critical and need added protection and which devices are unsafe and should be kept off the network.

Additionally, IoT and OT devices typically lack the ability to support certificates and other forms of advanced authentication that are taken for granted in laptops and servers. As a result, organizations often must simply whitelist these devices based on MAC address. Ultimately, organizations are forced to manually define what the IoT devices are and then again manually manage a fleet of "exception" devices that are blindly trusted in the network, which defeats the point of NAC in the first place.

2 It Can Be Hard to Define and Audit IoT Policies With NAC

One of the most consistent goals of a NAC deployment is to put devices into logical groups based on the posture and role of the device. However, this is yet another challenge when it comes to IoT devices. Unlike a general-use laptop, IoT devices often have much more narrow uses and behaviors. IoT devices may have vulnerabilities or limitations that make them hard to patch, and often it is not practical to take an an IoT device out of service if there is an issue. For example, a hospital can't simply disconnect a critical medical device or an elevator. As a result, IoT devices typically need to be tightly isolated, ensuring that they can talk to the few systems that they need, but are protected from the widespread access that could lead them to being compromised.

To build appropriate isolation policies, organizations will need to know the unique requirements for a particular device such as how it's actually behaving and what it is communicating with. For example, example, video cameras need to communicate to a camera management system. Medical imaging devices need to communicate to a central PACS or DICOM server. Every type of device is different and communicates in a unique way. To protect IoT devices, you need to build this "allow list” of communications.

Unfortunately, NAC solutions lack the fundamental visibility needed in order to build appropriately fine-grained segmentation policies, and do not have an understand of what is normal/baseline versus abnormal. Instead, teams can be required to manually learn and map out the specific needs of each device. Enforcing those policies will require managing detailed allowlists for each device type on each switch. Even when the policies are created, there are few options to audit the policies to make sure that things are behaving as expected. In short, it becomes a large amount of manual work for IT and security staff with many opportunities for mistakes that could leave a device exposed or break its functionality.

3 Enforcement is Often All Or Nothing

As the name makes clear, the overarching goal of NAC is to control access to the network. The ability to provide pre-access enforcement is one of the unique and most important traits of NAC. However, this core goal can also be one of the most elusive in real-world practices in that it is largely an all-or-nothing proposition.

Typically, NAC will be applied to a sizable section of the network such as a building. However ,that building will likely contain a wide variety of devices and systems such as building facilities, physical security devices, regular end users, guests, workgroup devices, and many more. Since NAC is a pre-access control solution, organizations must cover ALL the switches and the wireless infrastructure in the building at the same time or any unaddressed devices will be blocked by default. This means teams must prepare for the challenge of figuring out what policies to use for all the devices in the building, which can be varied and diverse. To reduce the chances of breaking things, organizations rely on extensive monitoring and testing phases, which can last for months, years, or in some cases simply remain indefinitely. This can result in organizations spending a great deal of effort without ever seeing the return on their investment.

A more practical approach is to start with specific systems or use cases, and gradually role out an access policy over time. For example, with an IoT purpose-built platform based on real-time traffic analysis, an organization could choose to focus on protecting security cameras one month and then HVAC systems the next.

4 Misses Threats and Risk After Access

NAC solutions enforce initial access decisions, but do not ensure that a device doesn’t do bad things once that access is granted. The decision to allow access is often based on fairly straightforward device traits. Does the device present the correct cert? Is the MAC address recognized? Does the system have the last AV updates? This naturally helps to control the risk of devices connecting to the network.

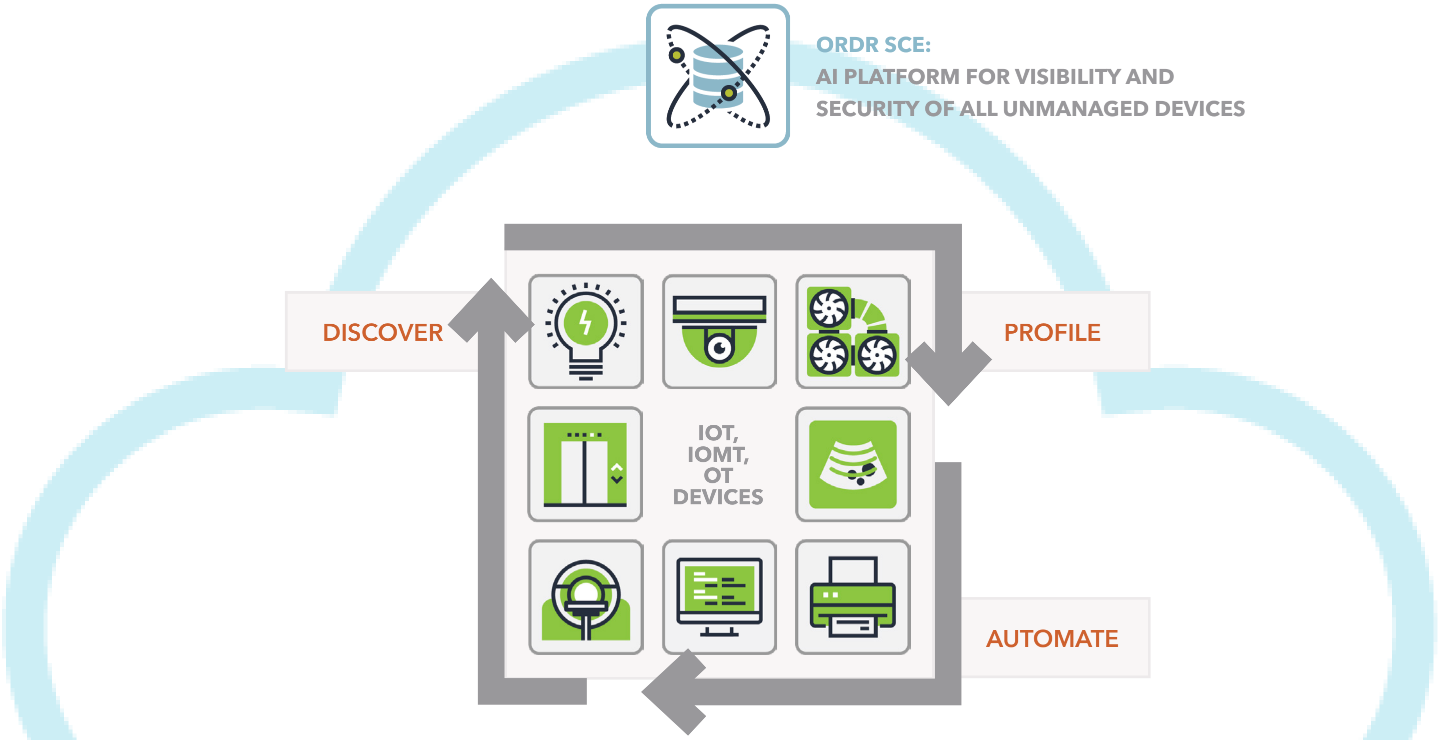
However, a device that is already compromised or is compromised post access poses by far the greatest risk to the network, and this is where NAC typically struggles. A device that is compromised by malware may still pass all of the pre-access checks. Detecting malicious behavior and signs of compromise often requires ongoing continuous analysis of the device’s behavior and traffic. Likewise, attackers may often try to spoof the identity of a device in order to evade controls. For example, a device may present itself as an IoT device, but its behavior may reveal that it is actually a laptop.

Detecting these types of threats and evasion requires a different type of visibility and analysis than what NAC provides. NAC naturally makes point-in-time access decisions based on set criteria. It doesn’t provide ongoing traffic analysis to verify behavior and identify threats. In many cases, organizations will need both.

How Ordr Delivers Visibility And Security for IoT and Unmanaged Devices

The Ordr Systems Control Engine (SCE) lets organizations quickly and safely gain visibility and control over all devices in their environment. Ordr can provide a standalone solution for device security or can provide a natural complement to a NAC deployment to help avoid the issues we've discussed in this document.

As shown in Figure 1, Ordr delivers the complete device security lifecycle – from discovery and classification to risk assessment and segmentation.


ORDR SCE:
AI PLATFORM FOR VISIBILITY AND
SECURITY OF ALL UNMANAGED DEVICES
DISCOVER
PROFILE
AUTOMATE
IOT,
IOMT,
OT
DEVICES

DISCOVER ALL DEVICES

- Agentless deployment
- Classify by make, model, serial number, location, O/S
- Vulnerabilities, exploits, FDA recalls
- Weak ciphers/certificates

BEHAVIORAL PROFILE DEVICES

- Baseline communications
- Visualize via VLAN and network arch
- Anomalous and malicious communications
- Understand utilization

AUTOMATE ACTION

- Trigger workflows for CMMS, CMDB
- Proactive segmentation and enforcement on NAC, FW, switches
- Incident response segmentation for vulnerable devices

FIGURE 1: ORDR DEVICE SECURITY FRAMEWORK

First, Ordr takes an agentless, passive approach to visibility. The platform passively monitors all traffic in the environment and uses industry-leading artificial intelligence to automatically identify every device based on device traits, traffic analysis, and device behavior. Ordr Flow Genome then maps out the traffic flow "genome" for every device, revealing exactly how and with whom a device needs to communicate. At a bare minimum, this provides the prerequisite visibility that teams will need before deploying NAC-based policies.

Next, Ordr can use this visibility to automatically generate microsegmentation policies based on the actual needs of each device. These policies ensure that things don't accidentally get broken by ensuring devices have access to systems they need, while simultaneously reducing their exposure to the bare minimum.

Lastly, Ordr continuously monitors the traffic and behavior of the devices to identify signs of a threat. Analysis can reveal anomalous behavior or interaction with malicious domains or IP addresses that could indicate that a device is compromised. By constantly analyzing the traffic and behavior of devices, Ordr can likewise identify devices that are attempting to spoof their identity. Collectively, these capabilities allow organizations to easily gain visibility control over their environment and quickly see a return on their security investment.

Conclusion

With the explosive growth of unmanaged and IoT devices, organizations need to consider the best way to secure them. While NAC can play an important role in the overall cybersecurity of an organization, it may not be the right fit when it comes to securing unmanaged devices. A purpose-built platform like Ordr however easily discovers, classifies and maps communications patterns for all IoT devices. Risk assesment can be performed and dynamic segmentation policies can then be created to isolate vulnerable devices. If you would like to learn more, please reach out to the Ordr team at **www.ordr.net**.