Accelerating Your NAC Deployments With Ordr

Do you already have a NAC solution deployed or are considering one? Network Access Control (NAC) can play a powerful role in an organization's overall cybersecurity strategy. Network Access Control solutions "support network visibility and access management through policy enforcement on devices and users of corporate networks." This means that a single, comprehensive software layer across all points of network entry serves as a sort of security guard, denying or allowing access based on who, or what is requesting access.

However, as many who have deployed NAC can attest, you can run into potential challenges along the way. NAC solutions in particular, are very strong at user and managed device authentication, but have limitations in specific areas – visibility into IoT and unmanaged devices, NAC for wired neworks, monitoring for threats post access, enforcement policy creation and the challenges with bringing people, process and technology together.

In this whitepaper you'll learn how to accelerate these deployments using Ordr.

NAC Deployment Challenges

Let's take a look at a few of the top issues that organizations typically face with NAC deployments:

1

Lack of Visibility into IoT and Unmanaged Devices

The rise of IoT and OT devices is often cited as one of the drivers behind the adoption of NAC. However, NAC was initially targeted towards users or devices that could authenticate to the network and is actually a weak solution for non-user devices. IoT and unmanaged devices almost always lack the ability to support certificates and other forms of advanced authentication that are taken for granted in laptops and servers. Additionally, by their nature, these devices lack agents or ability to be patched or secured with security agents. Traditional NAC profiling offers insufficient visibility and context on these devices to confidently apply policy decisions.

As a result, these devices are often simply allowed based on MAC address, IP, or some other basic identifier. Organizations quickly grow a fleet of "exception" devices that are blindly trusted in the network, which defeats the point of NAC in the first place. What organizations actually want is visibility into what the IoT devices actually are, and the ability to link "what they see are connecting" with what they have in their CMMS/CMDB so they can:

- confirm they are owned assets
- track the usage of these devices and create an inventory data lake for use across multi-department tooling (OT team, IT, InfoSec)

NAC is just incable of doing this.

RESULT: NAC deployments stalled due to lack of visibility into IoT and unmanaged devices.

2

Challenges with NAC for Wired Networks

Many customers have successfully deployed NAC for wireless deployments. Wireless solutions come with integrated clients and the authentication process is easy. In stark contrast, NAC for wired networks have been a challenge.

Organizations have problems taking a fully working network of heterogenous devices and users, and introducing authentication and access control. Often, the nature of clients is so diverse that organizations have major challenges establishing fundamental configs they can support. The other challenge is with unknown device access control; organizations ofen seek minimally disruptive options such as MAC Authentication Bypass (MAB) that allows network access solely on the virtue of a recorded MAC address, but this then introduces the issue of a fleet of "exception devices" blindly trusted in the network (as referenced earlier).

A hard-line NAC approach where devices are not allowed by default (guilty until proven innocent) is often disruptive to critical services and productivity. This can be especially challenging in certain verticals like healthcare where network disruption can cause more than just financial cost or compromise of intellectual property or productivity.

RESULT: NAC deployments stalled to due fears or actual bad experience with service disruption.

3

Monitoring For Threats and Risks Post Access

NAC solutions do their best work when making initial access decisions based on fairly straightforward device traits. Does the device present the correct certificate? Do I recognize this MAC address? Does the system have the last AV updates? This naturally helps to control the risk of devices connecting to the network.

However, NAC isn't effective in detecting threats and risks post access. Detecting malicious behavior and signs of compromise often requires ongoing continuous analysis of a device's behavior and traffic. 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.

RESULT: NAC deployments stalled because of lack of ability to continuously analyze risks

4

Inability to establish enforcement polices for unmanaged devices

Even for devices that are trusted or classified, understanding what to permit or deny and where is a major hurdle that most NAC customers grapple with. Unmanaged devices – IoT, OT or IoMT – rely on specific communications to function. For example, video cameras need to be connected to a camera management system. Medical imaging devices need to communicate to a central PACS or DICOM server.

This means that policies need to be created that ensure these devices remain tightly isolated, while ensuring they have access to the truly essential services they need. This can create enormous complexity since the specific needs will vary from device to device and allow list will need to be managed on each switch.

Traditional methods of performing exhaustive flow and packet analysis – traffic captures, firewall/ACL logging, neetflow analysis– are too manual and time-consuming to keep pace with the dynamics of a hyper-converged network. This often leaves organizations with a choice between two poor options when it comes to policies for unmanaged devices. Either allow them into the organization, or build very complex policies that are hard to manage and risk breaking things.

RESULT: NAC deployments stalled because policy creation is too challenging and time-consuming.

5

NAC deployments are often stalled by people and process

NAC entails collaboration from multiple teams and solutions. The issue is that NAC is typically an all or nothing proposition. Therefore, network equipment, policy servers, software versions must all be upgraded to suport NAC. This means significant costs in hardware and software, but also requires intensive labor to do this. Integration is required between different services and many solutions such as Active Directory, networking equipment configurations, certificates, MDM, AV/Servers, client software are required for a successful deployment. NAC is not a drop-and-insert technology. It ends up touching everything so everyone must get involved. If one piece of the NAC solution fails, access for a vast number of users and devices can be impacted.

Organizations want to "incrementally" deploy NAC to protect the environment by segmenting the network once workstation policies are completed and users are authenticated. But NAC is an all-or-nothing solution; it cannot support incremental segmentation based on unmanaged/IOT device criticality.

RESULT: NAC deployments are often stalled by people and technology

Addressing NAC Deployment Challenges With Ordr

Ordr can accelerate NAC deployment challenges, in particular with the visibility and security for unmanaged and IoT devices. Ordr can address the following:

- What is on the network?
- What is it doing on my network after it connects?
- Is it at risk? Is it infected or have vulnerabilities? Has it been recalled?
- Is it compliant? Does it have security software installed with current patches, etc? Does it have weak ciphers and certificates? Is it spoofed?
- Is it behaving normally for this device profile? Is it communicating to a malicious domain?
- How can create policies to segment high-risk 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.

First, Ordr takes an agentless, passive approach to visibility. Ordr Systems Control Engine 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 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.

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.

NAC Deployment Challenges

Lack of visibility into unmanaged and IoT devices

ORDR SOLUTION: Ordr provides high-fidelity discovery and classification into devices – make, model, serial number, location and more. Ordr also integrates with external threat, vulnerability and manufacturing device databases to enrich device data. This rich context on devices can be shared with CMDB, CMMS, or NAC solutions to allow or deny access to devices.

Fears of service disruption with wired deployments

ORDR SOLUTION: Ordr facilitates a phased approach of NAC deployments, with increasing segmentation and control. For example, networking and security teams can use Ordr to enable segmentation of IP cameras one month and then HVAC systems the next month. Segmentation is easy because dynamic policies can be generated with the Ordr platform

Deployments stalled by people and process

ORDR SOLUTION: Ordr delivers one common platform which provides critical information for security, networking and device owners. Role-based access control enables appropriate access to different dashboards and functionality for different users. In addition, the Ordr deployment is also passive and agentless, thus minimizing the requirements and impact to different teams.

Lack of ability to continuously analyze for risks

ORDR SOLUTION: Ordr Flow Genome maps and baselines all device communications, and provides continuous monitoring of device behavios and their risks. When a security threat is detected, Ordr triggers the appropriate incident response workflows and enables rapid containment through automated segmentation policies and enforcement on existing NAC, firewall or network controls.

Policy creation challenging and time-consuming

ORDR SOLUTION: Ordr alleviates these challenges by analyzing device behavior to establish group and device-centric baselines unique to each customer's network. These "sanctioned" communications patterns can be dynamically converted into segmentation policy for one-click provisioning on NAC, firewalls and network.

Conclusion

As organizations look to bolster their security, NAC can play an important role in the overall solution. However, to get the most out of their investment in NAC, organizations need to be aware of the potential challenges that can hold their deployments back. This document brings some of these challenges into the light. However, the good news is that these problems can be addressed with Ordr. The Ordr platform will support and complement NAC. If you would like to learn more, please reach out to the Ordr team at **www.ordr.net**.