portnox™
boundlessly smart

DATA SHEET

THINK YOU'VE THOUGHT OF EVERYTHING?

Think again.

TOP 5 MOST COMMON NAC PITFALLS

Network access control isn't new. It's been around for a while and by now most enterprises have already had at least one attempt at deploying a solution to address the key questions of: *"Who is currently accessing my network?"* and *"Should they be there?"* NAC is successful only if it is accurate. Lack of accuracy means you'll be blocking the good guys, or worse, letting in the bad guys. It's just that simple.

The challenge is that most NAC solutions have proven far too complex to deploy, scale and manage. This means the information they yield is far too often stale or just plain incorrect. Common phrases heard during NAC post-mortem discussions are: *"too complicated"*, *"too strict"*, *"cumbersome"* and even *"inadequate"*.

This document outlines the common pitfalls of NAC deployments using the conventional solutions on the market today. To date, neither industry standard based approaches, such as 802.1X, nor proprietary specialized vendor solutions have been able to address the architectural limitations that keep NAC from delivering on its true promise.

THE QUICK LIST:

- Appliances Everywhere - Prepare to install a lot of hardware.
- Beware of 'Agentless' Claims - Things you won't see in the proof of concept or datasheets.
- The Curse of 802.1X - You don't need to take a dependency on such a complex standard.
- The Other Kind of MAC - It should'nt be this easy to bypass your defenses.
- What You're Still Not Seeing - All this, and you still can't see everything.

Appliances Everywhere

RISK: Many traditional NAC solutions require separate appliance deployments at each and every site to ensure those networks are visible and controlled. Not only does that mean a physical (or virtual) appliance at each location, it also means the technical resources to set-up, configure and manage. Most organizations end up deploying only in the main sites, leaving the network vulnerable at remote sites and branches and missing the complete picture of all users/devices, thereby greatly reducing the overall integrity and accuracy of their deployment.

SOLUTION: Consider solutions that offer a scalable and central deployment that can easily illuminate and remediate remote sites into a centrally configured and controlled solution. Avoid solutions that require independent deployments for each site. Ask the question and demand a clear answer on how the solution scales to provide visibility and remediation at remote offices and sites.

Beware of 'Agentless' Claims

RISK: Beware of "agentless" claims! Most solutions have updated their marketing to claim "agentless" functionality. The reality is they require agents for remediation once NAC starts enforcing a policy. In a typical network more than 60% of the devices aren't even able to run agents. Ultimately the agent becomes yet another means to manage Windows compliance – something for which you already have a myriad of better (and cheaper) tools.

SOLUTION: Verify that you can easily and accurately identity, authenticate *and* remediate without the need for agents. Remember that even if you're willing to accept an agent-based solution, it will only address a subset of your devices.

The Curse of 801.1X

RISK: Most NAC solutions require 802.1X to reach their full functionality. At the surface this seems like a great standards-based solution for NAC. In reality, 802.1X is an all-or-nothing solution requiring the deployment of Radius servers, PKI and user/device enrollment as well as all network hardware and devices to support a specific version/ configuration. For this reason, even enterprises with significant resources have relegated 8021.X for their wireless networks only. Extending to wired/Ethernet, VPN, or virtual networks is effectively impossible.

SOLUTION: Look for solutions that can either deliver their complete NAC functionality without an 802.1X dependency. Many of these solutions can also leverage any existing or future 802.1X environments, if needed.

USA tel. +1.855.4portnox | usinfo@portnox.com | 623 Eagle Rock Avenue, Suite 396, West Orange, NJ 07052
UK tel. +44.1273.256.325 | dotell@portnox.com | 5 Albourne Court, Henfield Road, Albourne, West Sussex BN6 9FF
ISRAEL tel. +972.9.957.9889 | tellus@portnox.com | Elbe House, 33 Ben Gurion St., Herzlia 46785

The Other Kind of MAC

RISK: Most all NAC solutions default to MAC address management far too often when agents or rights on the endpoint are unavailable. MAC addresses are inherently insecure, easy for anyone to find (simply look at the bottom of any laptop or phone). No vendor will make claims to using MAC addresses – but many will default to MAC address for unknown devices or "dumb" IP devices.

SOLUTION: Look at best practice guides and review default settings for policy. VoIP, IP Camera and printers are typically the first to receive entry to the network based on their MAC.

What You're Still Not Seeing

RISK: By design, the requirement to mirror ports and networks means that even the best NAC solutions are still ignoring the complete picture. Most provide only limited (if any) support for virtual networks (think datacenter and VDI) and only few consider the VPN and cloud networks part of their concern. This continues to erode the accuracy and integrity of the data provided leading to compromises on policy precision and tolerance.

SOLUTION: Only consider solutions that can easily traverse virtual networks, cloud (IaaS, PaaS) platforms as well as VPN segments. Future-proof your NAC and c¬¬hallenge the solution to go beyond the proof of concept and scale to address these environments with a complete feature set including full remediation.

Portnox Is Different

Portnox is accurate because it traverses all networking layers - Ethernet, wireless, virtual, VPN and even the cloud to illuminate, visualize, analyze and control all connected users and devices. It speaks directly and natively with all existing switches, wireless access controllers, routers and firewalls to get a complete, 100% accurate view of all devices currently connected to the network. Nothing can hide.

Instead of using agent software, it communicates natively with the connected devices to validate their type, compliance and identity. Taking accuracy a step further, it even communicates with user-driven devices such as laptops, desktops, VoIP phones, tablets, etc. to identify the user currently using the device. Every decision Portnox makes factors in the Device, Network and Identity (DNI). It even looks at a user or device's prior behavior just like a 'credit score' to ensure that only the right devices are allowed into the right segments of the network.

Portnox is a software only solution. No appliances are needed and no changes to networking infrastructure such as port mirroring or network taps are required. It scales easily across the enterprise and delivers the highest levels of accuracy and control.

USA tel. +1.855.4portnox | usinfo@portnox.com | 623 Eagle Rock Avenue, Suite 396, West Orange, NJ 07052
UK tel. +44.1273.256.325 | dotell@portnox.com | 5 Albourne Court, Henfield Road, Albourne, West Sussex BN6 9FF
ISRAEL tel. +972.9.957.9889 | tellus@portnox.com | Elbe House, 33 Ben Gurion St., Herzlia 46785