portnox™
boundlessly smart

WHITE PAPER

THINK YOU'VE THOUGHT OF EVERYTHING?

Think again.

TOP 5 MOST COMMON NETWORK ACCESS CONTROL PITFALLS

Network Access Control (NAC) isn't new.
In fact, it's been around for over a decade 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 the bad guys in. 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 This means the information they yield is far too often stale or outdated. 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 available on the market today. To date, no on-prem solution based on an industry standard, 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.

Portnox NAC is accurate because it traverses all networking layers - ethernet, wireless, virtual and VPN to illuminate, visualize, analyze and control all connected users and devices. It speaks directly and natively to 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 appropriate 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.

1 Appliances Everywhere

PITFALL: 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 these appliances needs to be put in place. Most organizations end up deploying only at the main sites, leaving the network vulnerable at remote sites and branches, missing the complete picture of all users/devices. This thereby greatly reduces the overall integrity and accuracy of their deployment.

SOLUTION: Consider solutions that offer a scalable and central deployment methodology 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.

2 Use Agents With Caution

PITFALL: Agents are good for continuous monitoring, especially for the mobile workforce and for VPN access. But for many internal LAN scenarios, you should go with an agentless approach. The variety and quantity of endpoints in your internal LAN will usually dictate that. Be agentless until you have to have an agent. Beware of “agentless” claims! Most solutions have updated their marketing to claim “agentless” functionality. The reality is that they require agents for remediation once NAC starts enforcing a policy. Without these, policy enforcement decisions that aren’t automatically remediated result in prolonged disconnection and helpdesk costs. Another common misleading sales pitch entails solutions that actually use a technique of copying over an unsecure NTLM based RPC agent, executing and then deleting it. Besides the additional network traffic burden, they actually expose your network by using unsecure NTLM based RPC protocols.

SOLUTION: Verify that you can remediate without agents. Remember that even if you’re willing to accept an agent-based solution, it will only work on supported devices. Verify that an agentless solution does not require unsecure NTLM based RPC, or other unsecure protocols.

3 The Other Kind of MAC

PITFALL: Most NAC solutions default to MAC address management far too often when agents or rights on the endpoint are unavailable. MAC addresses are inherently insecure and easy for anyone to find (simply look at the bottom of any laptop or phone). No vendor will openly discuss using MAC address, but many will default to MAC address for unknown or “dumb” IP devices. Managing MAC address exceptions is a never ending task, resulting in a huge daily burden.

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

4 Be Cautious of 802.1X

PITFALL: 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 a good fit for limited environments such as wireless. It can also work well in a very homogenous wired environment which is consisted of mostly managed endpoints. Most 802.1X based solutions will also force you into 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 802.1X for their wireless networks only. Extending to wired/ethernet, virtual networks is effectively impossible with on-prem solutions.

SOLUTION: Look for solutions that can 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. Or, look for solutions that can provide you with the flexibility to deploy 802.1X from the cloud, where the infrastructure complexity burden is lifted.

5 What You’re Still Not Seeing

PITFALL: By design, the requirement to mirror ports (span ports) means that you will lose some network packets even with the strongest appliance. That also means that you won’t be able to use this technique remotely with remote branches. Supporting only new switches, or certain vendors means that either you see only part of the network now or in the future, when working with other vendors. Not supporting virtual environments might be another possible blackspot.

SOLUTION: Only consider solutions that are vendor agnostic, and can traverse up to the virtual network. Future-proof your NAC and challenge the solution to go beyond the proof of concept and scale to address these environments with a complete feature set over all environments.

portnox™
boundlessly smart