Portnox NAC

On-Premise Solution Overview

CONTENTS

AT A GLANCE

- Centrally Managed
- No Agents
- No Infrastructure Changes
- No reliance on 802.1X
- Covers ALL Access Layers
- Covers ALL Devices
- Real-time/Event Driven
- Scalable
- Easy to Manage
- Flexible & Deployable

"We are proud to present Portnox our 2016 Strategy, Innovation, and Leadership Award for Network Access Control (NAC)"

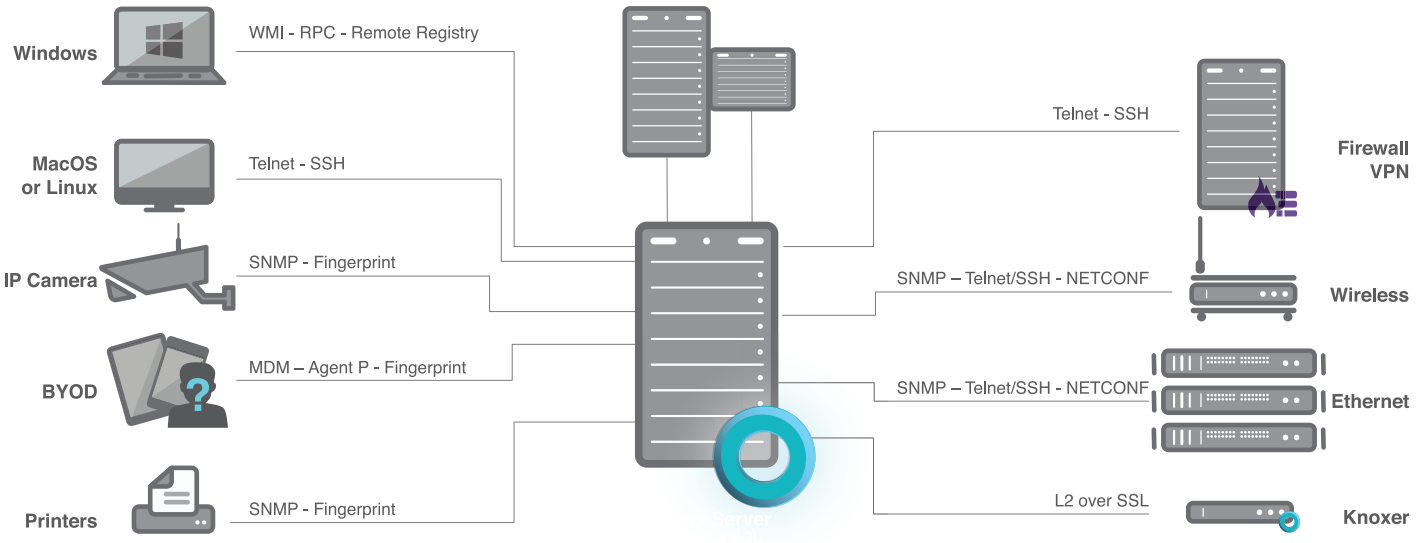
Joe Fristensky. Partner and Vice President. Frost & Sullivan

Technology Introduction

Portnox provides complete Network Access Control across wired, wireless, VPN, virtual and even cloud resources. Unlike most other solutions, Portnox does not require appliances, agent software, 802.1X or changes to existing networking infrastructure such as mirror or span ports. It supports all existing networking infrastructure and is uniquely adept at handling a wide variety of devices with varying levels of IP support.

In essence, Portnox is a software based solution that runs on Windows Server (2008R2 or 2012) to continually communicate with all existing networking infra-structure to gain complete visibility into all assets currently connected to the network. This is achieved through a variety of connectivity options including SNMP, telnet, SSH, etc. With this, definitive and highly accurate view of the network (after all, devices can escape an IP range scan, but not an ARP table), Portnox is now able to interrogate each and every connected device to verify its type, level of compliance, identity and even the identity of the user. All this is done without the use of agent software but instead leveraging over twenty five different methods of profiling and authentication ranging from WMI, remote registry and named pipes for Windows devices, SSH and Telnet for MacOS and Linux devices and many others for the wealth of non PC devices that comprise today's network. Portnox then correlates the data it finds to ensure that each policy can determine which device, at what level of health/compliance, with which specific user (or group of users) can connect at each specific location.

Portnox Architecture Summary



Portnox Architecture Diagram

Unlike many traditional NAC solutions that rely on port mirroring, IP range scans, inventory directory or some other passive non-real-time method to gain device visibility, Portnox directly connects via native protocols to your network infrastructure (switches, WLC, VPN, virtual) to provide real-time immediate awareness of network changes. For example for managed switch-es, Portnox will most typically connect via SNMP (read & traps) — this assures Portnox is immediately aware of changes at the switch level. When a new device connects to a port, Portnox is aware, often before it has an IP!

Portnox then connects to configured “ip helpers” (router/firewall) to gain addition device knowledge via ARP tables and other information. With this initial device knowledge and profile, Portnox will attempt to authenticate the device (see Authentication page 4) to confirm it is a valid corporate device or designate the device as rogue (see Enforcement page 5).

With Portnox nothing can hide — if a device is connected to your network and has power, Portnox is aware. Portnox will make you aware of devices on your network connected to switches that Portnox has not been configured to manage — Portnox monitors link ports and will notify of such devices in our network clutter view. With Portnox, nothing can hide!

Portnox is a software-based solution that deploys on windows 2008/2012 R2 server(s), physical or virtual. Portnox deploys at a single location providing NAC across the entire enterprise. For those environments that require based on business reasons or network topology a distributed deployment, Portnox supports this at no additional cost.

ARCHITECTURE HIGHLIGHTS

- Natively Connects to network infrastructure elements
- No Agents to deploy
- No reliance on the complexity of 802.1X
- Real-time, event driven device awareness
- Software based, No Appliances
- Central or distributed deployment based on your needs at no additional cost.

NOTHING CAN HIDE

- Discovery starts at the infrastruc-ture layer
- Real-time/Event driven
- Continuous
- No passive IP range scans, port mirroring
- Easily create device filtered views based on many device attributes including OS, applications, loca-tion, security status and more

Device Discovery (real-time, continuous)

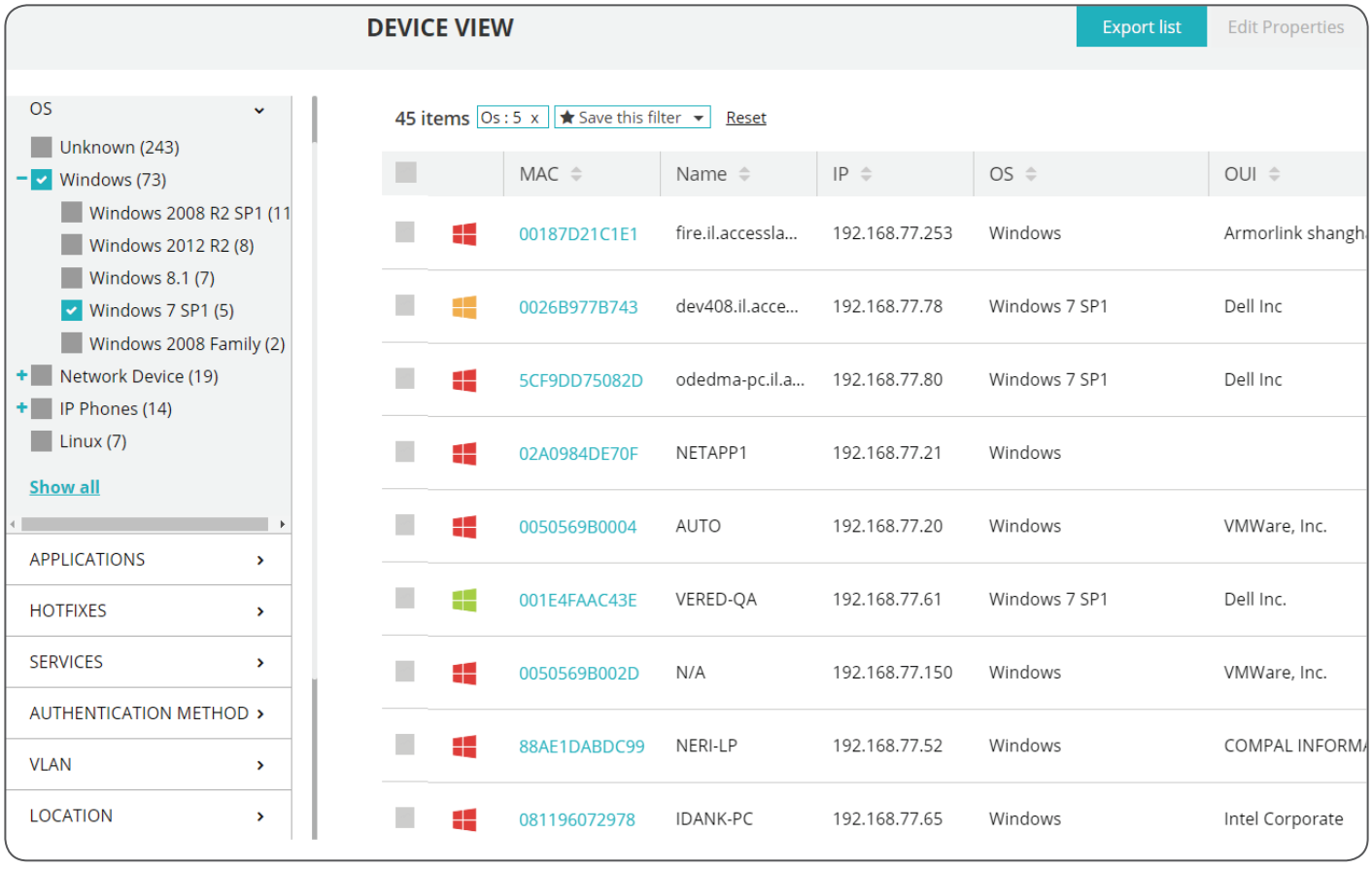
As previously discussed, Portnox starts at the infrastructure layer. Connecting directly to your wired, wireless and virtual infrastructure, Portnox delivers real-time, continuous and event driven illumination of any and all devices connecting to your network.

Portnox does not stop at initial device connection, configuration options sup-port continuous validation of devices previously validated to assure they maintain compliance while connected to the network.

Converged VoIP environment? No problem, Portnox will automatically detect, discover and validate separately VoIP phones and connected device.

Concerned about unauthorized hubs or access points? No problem, Portnox discovers, notifies and can take action against unauthorized hubs or access points. If authorized, Portnox provides discovery, authentication, and control for each device independently.

Portnox device view provides a configurable view with easy filtering options to narrow your view based on OS, application, services, authentication meth-od, security status, service, hotfixes and more. Want to know all connected devices running Windows SPI — just click, view and easily export!



Device Authentication

Win32	[kerberos]	[ntlm2]	[registry]	[workgroup]
Unix & Linux	User Pass [ssh]	Key Auth [ssh]	SSHD FP	[telnet*]
Printers	[snmp]	[Oil lookup]	http	3D
Fingerprint	[proprietary]	[dhcp]	[syn/arp]	[salt]
VoIP	pbx	VMware	VPN	Geo IP
Interactive user	[portal]	[chaperone]	[voucher]	[guests]

Sample Device Authentication Methods

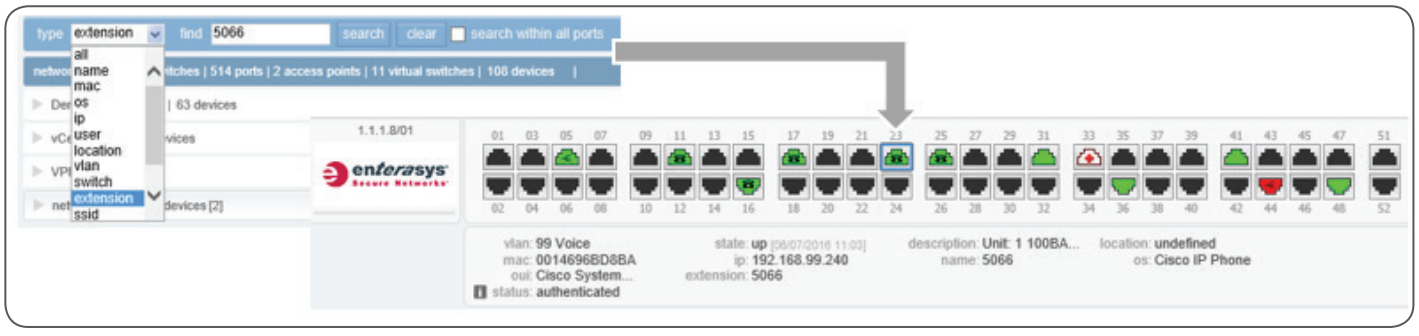
Once discovered, the next step is authentication. As with infrastructure connectivity, Portnox authenticates corpo-rate devices natively without the need for any agent, supplicant or “dissolvable” agents. Portnox supports over 25 authentication methods to assure only valid corporate devices connect to the network, from common AD/domain to SNMP, SSH and our unique signature/finger print (OSFP) supporting secure, strong authentication of the grow-ing Internet of Things (IoT) devices.

802.1X or other agent based solutions have limited device support and as a result, for many devices including the growing IoT, will default to MAC address whitelisting, which not only creates significant management overhead, it is one step above doing nothing! Most all IoT devices have their MAC address on a visible label and even the most junior of hackers can spoof a mac address. Beware of any solution that defaults to MAC address whitelisting.

Portnox goes the extra mile, for example in a VoIP environment, Portnox not only provides strong authentication (typically via SNMP or OSFP), Portnox also integrates with the VoIP PBX to obtain addition details on the VoIP device in-cluding extension number — this information then becomes available and searchable. Want to know where VoIP extension 5066 is connected, with Portnox, it’s a click away!

AUTHENTICATION VALUES

- 25+ Authentication Methods
- No Agent
- No Suplicants
- No “dissolvable” Agent
- Strong, Secure Authentication for growing IoT devices
- Voucher for time limited device authentication



Enforcement & Compliance

Let's be honest, there are various solutions and methods for discovering de-vices connected to your network — the value of NAC is being able to proac-tively take enforcement actions for those devices that do not belong on your network or are not within your security or compliance risk tolerance. The problem is, most traditional NAC solutions do not have the level of device awareness or enforcement flexibility required for companies to trust moving to full enforcement. There are numerous network administrators and security officers with "arrows in their back" because a NAC solution blocked a critical valid device or failed to block an unauthorized device. That only has to occur a few times before enforcement is disabled and the NAC becomes just anoth-er discovery solution.

That is not the case with Portnox — over 80% of our customer deploy with full enforcement enabled. Why? Simple, device awareness, knowledge and enforcement flexibility!

We have already covered how Portnox works from the infrastructure layer up and that Portnox "goes the extra mile" by integrating with your PBX, AD and other device knowledge bases to gather as much detail on the device as pos-sible. A level not achieved by traditional NAC solutions.

Portnox also connects back to corporate PC(s) without any agent to compliance validate the device against a wide variety of checks including OS, AV, active NIC(s), local user privileges, removable storage, authorized (or unauthor-ized) programs, services and more. And if you already have an endpoint compliance validation solution, no problem, Portnox can check it's view on device status as part of compliance validation.

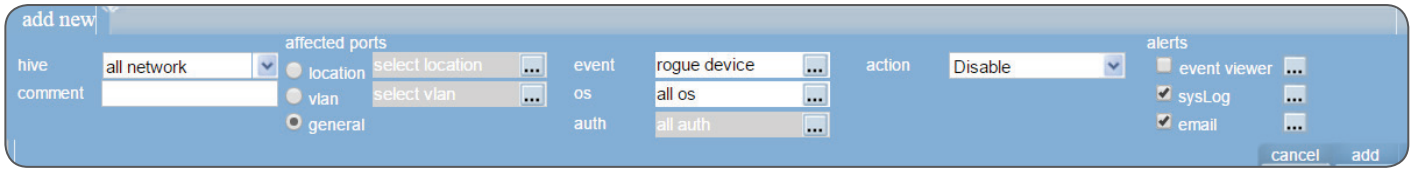
What truly separates Portnox is the FLEXIBILITY Portnox offers in what enforcement actions should be taken based on the device, user, authentication, location and compliance. Flexibility is critical to meet a companies balance of security and productivity. Maybe you would like a different enforcement action if a PC connects without AV in-stalled vs. AV installed but not updated? Or maybe you want more strict enforcement on devices connecting to your HR or manufacturing VLAN vs. the general office VLAN? Or you want to be sure any device connecting to conference room ports only have access to the guest VLAN.

ENFORCEMENT

- Flexible enforcement actions based on device, user, location, authentication, compliance
- Detailed endpoint compliance checks and validation
- Easily phase in enforcement to assure success
- Easily aligns to your balance of security and productivity

Portnox flexibility extends to device on-boarding, supporting pre-connect, post-connect and a hybrid partial pre-connect onboarding model and you can select different methods for different network segments, VLANs or groups.

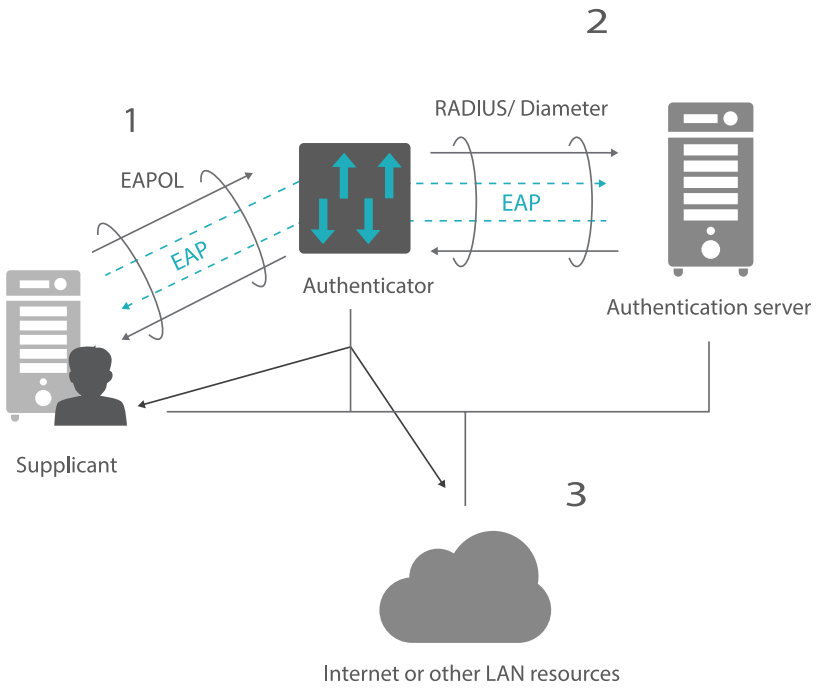
Finally, Portnox flexibility extends to your roll-out and migration from discovery to enforcement — start in monitor/discovery mode, slowly roll-out automated enforcement to specific ports, switches, VLANs or locations.



Easily set event actions based on network segment, location, VLAN, group and more

802.1X CONCERNS

- Very Complex and resource Intensive (pre and post)
- Hard to debug client connectivity issues. Help desk drain.
- Requires MAC address white listing for IoT and other unsup-ported devices
- Vendor sensitive to updates, upgrades, etc.
- Lacks advanced client compliance validation



Beware of 802.1X

Most all infrastructure vendors offering a NAC solution and many pure-play vendors will at their foundation re-quire 802.1X as their method to provide device authentication and access control, which are the two security val-ues provided by 802.1X, at least in theory. We say in theory because for many organizations the level of effort, time and expertise need to effectively deploy 802.1X enterprise-wide across wired and wireless networks is often unattainable. Unless you have several “IT Mac Gyvers” on staff with lots of free time you should think everything through before you drop into the 802.1X abyss.

Looking at 802.1X over your wired network, the first challenge is just the complexity of 802.1X. You have three major components to consider and configure often from different vendors: client devices, switches, and the radius server. And do not forget the growing number of IoT devices that will not support an 802.1X supplicant — get ready to manage a growing list of MAC addresses, and welcome the exposure to MAC address spoofing, but I di-gress. With so many dials to turn and elements to manage, the chances of something going wrong is almost 100%.

So, be prepared to spend many of man hours going through logs to try and debug the numerous issues you will face given the number of moving parts. Another side note — make sure your network engineers read up on PEAP, EAP-TTLS, and PKI, if not already knowledgeable, they will be at the expert level if/when they do finally fully de-ploy 802.1X.

The next challenge is with the client. As already mentioned, for the growing number of IoT devices that need net-work access and cannot support 802.1X — start logging their MAC addresses. But lets focus on those devices that can support an 802.1X supplicant. First, determine how you want to approach continued configuration and man-agement of all the client supplicants. Not only are you talking about different vendors, often within a vendor, a device upgrade can make changes to the supplicant. With 802.1X if you have a client connection problem, it is very difficult to determine where the issue resides as the client is not authenticated to the network. Get ready for an influx of help desk calls!

Should you finally get some devices working properly and reach enforcement/access control — make sure you have the help desk resources to manually on-board those valid devices that are blocked. With 802.1X there is no automated method to re-authenticate a device!

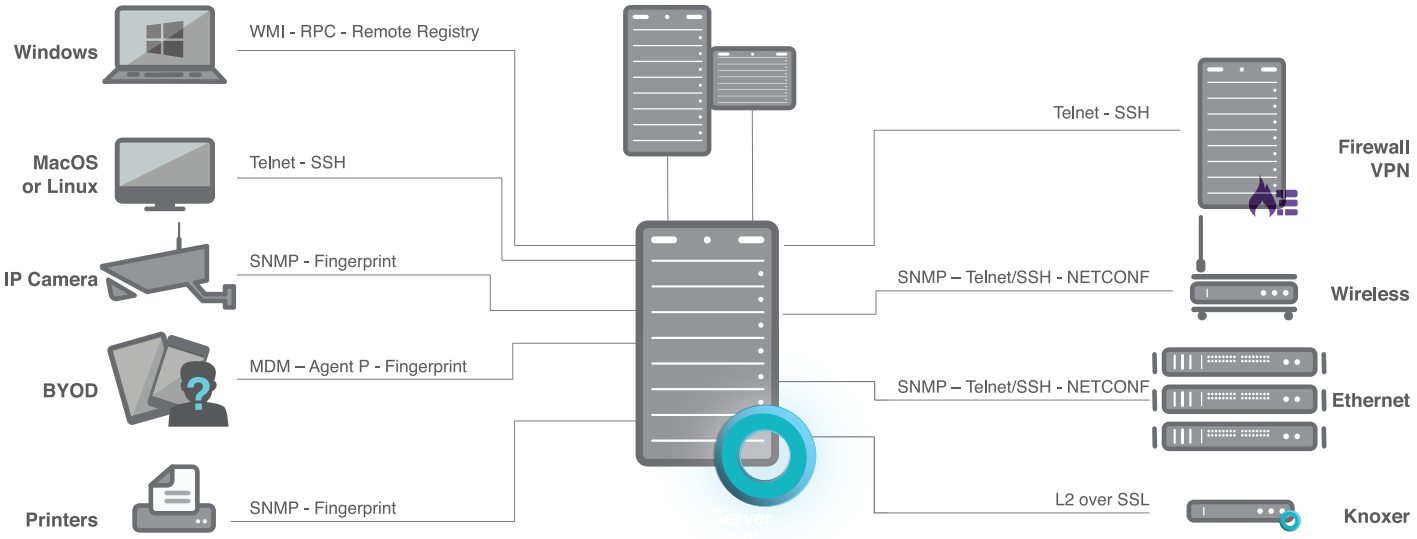
Before you go down the 802.1X path, consider a Portnox POC — side by side with your 802.1X solution of choice and see the difference first hand!

Portnox Is Different

Organizations of all sizes should have real-time clear visibility and control of all devices connecting to their network. The only question is how best to ac-complish this goal.

At Portnox, we focus on only one thing — that is to deliver network access control solutions that provide 100% visibility and control of any/ all devices over all your networks (wired, wireless, VPN, virtual). With a focus on ease-of-use, easy of deployment and flexibility, our solution is deployable, affordable and scalable across any sized company.

But, words are easy to write — our preference is that you see the Portnox first hand. Just email or give us a call and we can set up a quick demo or on-site POC.



portnox™
boundlessly smart

Contact Us
Americas usinfo@portnox.com | 1-855-476-7866
Europe dotell@portnox.com | (44) 1273-256325
Israel (972) 9-957-9889 | tellus@portnox.com