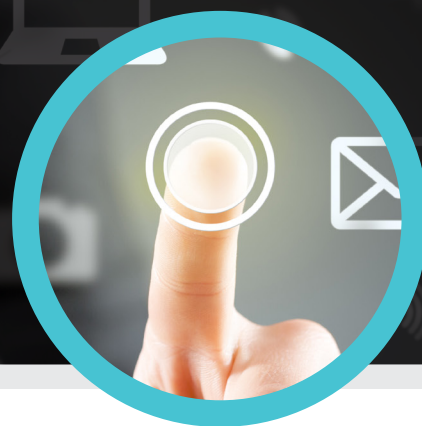# Portnox CLEAR™
Cloud Service

"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

Introduction

Today companies of all sizes are faced with the same security issues and growing compliance requirements as their larger counter part. PCI, SOX, HIPAA and others do not discriminate or make adjustments based on company size. The challenge for many is how to maintain a level of security and compliance even large companies struggle to attain but often with limited resources and budgets? As we will introduce in this overview, the answer for many is delivering Network Access Control (NAC) in the cloud!

The tremendous growth, acceptance and affordability of software as a service has brought economies of scale to all. Companies of all sizes are finally able to cost-effectively have access to enterprise-grade CRM, accounting, scheduling and other software and tools traditionally only affordable and deployable by large enterprises. The same should be extended to advanced security solutions such as Network Access Control (NAC). Traditional on-prem NAC solutions can bring a heavy cost in appliances and expert resources needed to properly configure and manage. As a result, for many organizations on-premise NAC solutions can often be out of reach in both cost and resource requirements. That is until now!

Portnox CLEAR delivers affordable, deployable and manageable NAC to any sized company as a cloud service. No appliances, heavy configuration or extensive expertise needed. Portnox CLEAR can be set up, configured and deployed in minutes!

This paper provides a high level overview of how Portnox CLEAR works and some of the key features and capabilities.
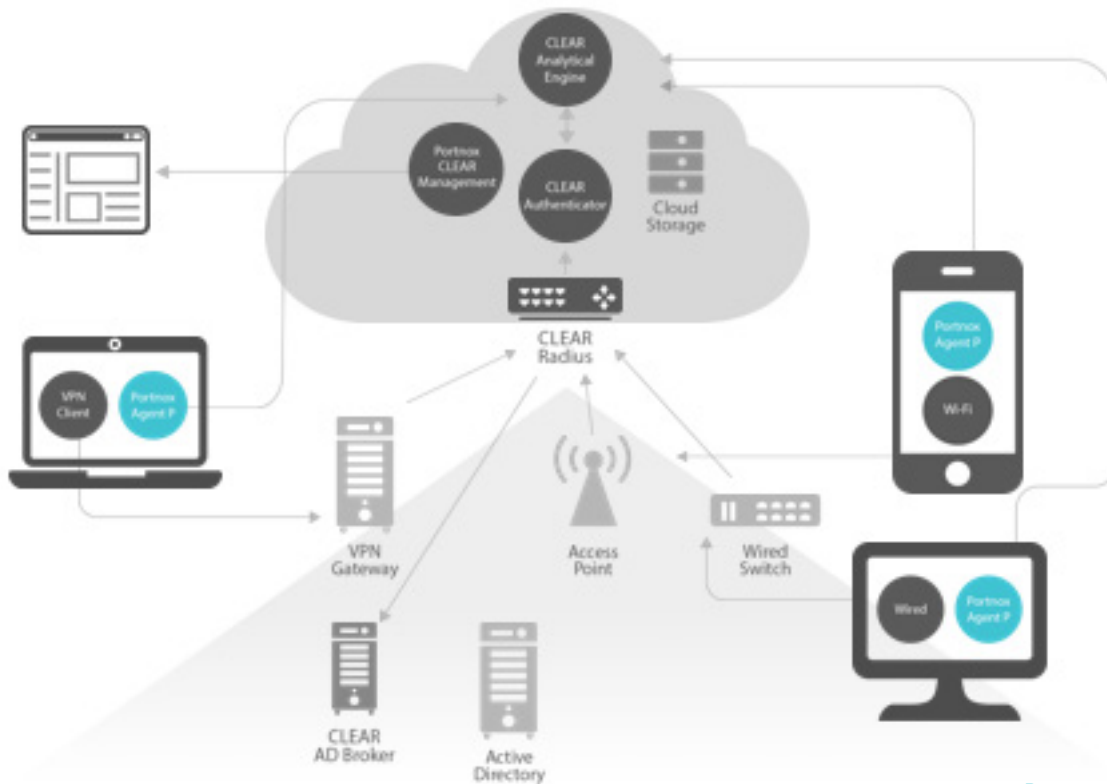
CONTENTS

AT A GLANCE

- NAC as a Cloud Service
- Continuous awareness of device risk posture
- Risk aware access controls
- Covers all access layers: wired, wireless, VPN
- Agent or Agentless deployment
- Automated push of wireless changed to affected devices
- Radius in the Cloud

Portnox CLEAR Architecture Summary

Portnox Architecture Diagram

Traditional 802.1X NAC solutions often bring a high cost and significant deployment and management overhead even to the most well seasoned and well staffed large enterprise. With Portnox CLEAR all the complexity associated with rolling out 802.1X, continuous wireless management and more is moved to the cloud, leaving the SME a quick, easy to deploy, easy to manage and cost effective NAC solution.

They key components that make up Portnox CLEAR include:

AgentP: Device agent supporting windows, MAC, IOS and Andriod devices.

CLEAR Radius: Cloud-based Radius Server & Authentication.

CLEAR AD Brooker: Options light-weight software to support AD authentication and access controls.

CLEAR Analytical Engine: Continuous awareness of device risk posture and alignment to policy.

CLEAR Guest Management: Optional add-on providing robust management and control of guest access.

Where many cloud-based access control solutions are focused only on wireless, Portnox understands a typical network often includes wireless, wired and VPN remote access. For this reason, Portnox CLEAR functions across all your access layers, wireless, wired and VPN! Why would you want a solution that only covers part of your network?

Portnox also supports none agent AD based authentication and options for MAC address management to support the growing Internet of Things (IOT) and devices that cannot support and agent or AD authentication.

ARCHITECTURE HIGHLIGHTS

o NAC delivered as a Cloud Service

o Continuous end-point risk monitoring

o Device Risk based access control

o Covers all access layers: wired, wireless, VPN

o Wireless management in the cloud

o Radius in the cloud

o AD integration

o Flexible Guest Management

Continuous Device Monitoring (AgentP)

At the core of Portnox CLEAR is AgentP, a light-weight agent available for windows, MAC, IOS and Android devices. Available for download from the Portnox CLEAR portal or associated appstore. Once installed, AgentP is easily registered via company email or active directory credentials depending on how the administrator configured CLEAR. That's it for the end-user/device — simple, easy and quick!

Once AgentP is enabled, it begins keeping a real-time and continuous posture assessment of the device. Depending on the device type, this will include such items as:

- Location
- Applications
- Encryption
- Anti-virus
- Firewall
- Updates
- Patches
- Jailbroken
- Rootkit
- Domain
- Certificates
- Open Ports

AgenP also provides device specific visibility including as shown below for a sample windows devices, details on security products, applications, users, network connections, hot fixes, certifications, services, peripheral devices and open ports!

DEVICE RISK MONITORING

- Continuous device risk validation on or off premise
- Supports windows, MAC, IOS and Android
- Easy to install and activate
- Device visibility & inventory
- Location aware

portnox™ CLEAR

DOWNLOAD PORTNOX™ AGENTP

Portnox™ AgentP provides information about your computer to your company's administrators.

| Download for **Windows** | Download for **Mac OSX** | Get on Store **iOS** | Get on Store **Android** |

DEVICES > DEVICE DETAILS

███████ @portnox.com   ██ 50

COMPUTER INFORMATION

|	
Manufacturer	LENOVO
Model	20AMS1FJ05
RAM	8,388,608 KB
Processor	GenuineIntel Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz
Domain membership	il.accesslayers.com (AD)
Device encrypted	No
TPM enabled	No
Windows Update	Automatically install

SECURITY PRODUCTS | APPLICATIONS | USERS | NETWORKS | HOT FIXES | CERTIFICATES | SERVICES | PERIPHERAL DEVICES | OPEN PORTS

Product Name	Type	Version	State
Windows Firewall	Firewall		Enabled
Microsoft Security Essentials	AntiVirus	4.10.0205.0	Enabled, UpToDate
Windows Defender	AntiVirus	6.1.7600.16385 (win7_rtm.090713-...	UpToDate
Microsoft Security Essentials	AntiSpaware	4.10.0205.0	Enabled, UpToDate
Windows Defender	AntiSpaware	6.1.7600.16385 (win7_rtm.090713-...	UpToDate

Items 25 ▾

Risk Aware Access Control

Most wireless solutions today will provide some level of device access control. Other solutions can provide knowledge and insight into a device. But being aware of the risk a device can pose to your network without delivering access control. Or managing device access without consideration of the device risk status are only partial solutions.

With Portnox you get both continuous real-time device risk-posture awareness and the ability to use that knowledge proactively as part of the access control decision. And not just for wireless connections, also for devices connecting through a port or even via your VPN. Portnox CLEAR also provides two-factor authentication for remote VPN connections.
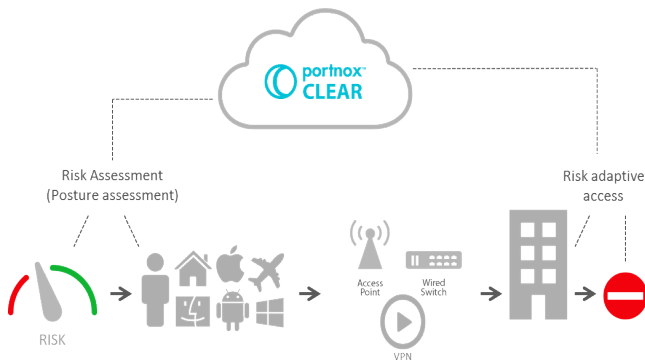
With Portnox CLEAR it could not be more simple to set your device type-specific risk attributes and access control policy. Based on the device type, you simply set a "risk value" to various attributes — for example for a windows device, you might set a risk value contribution for AV @ 50, missing patches contributes 80 and location is not a risk concern so it contributes zero.

The cumulative resulting value for a specific device represents the real-time, current risk score of that device.
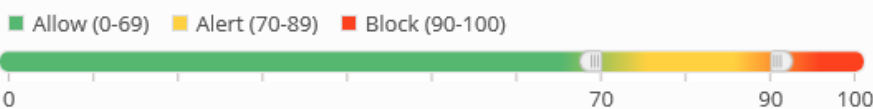
The access control/action policy is easily set by a simple slide bar to set your risk-based access control policy, allow, alert, block!
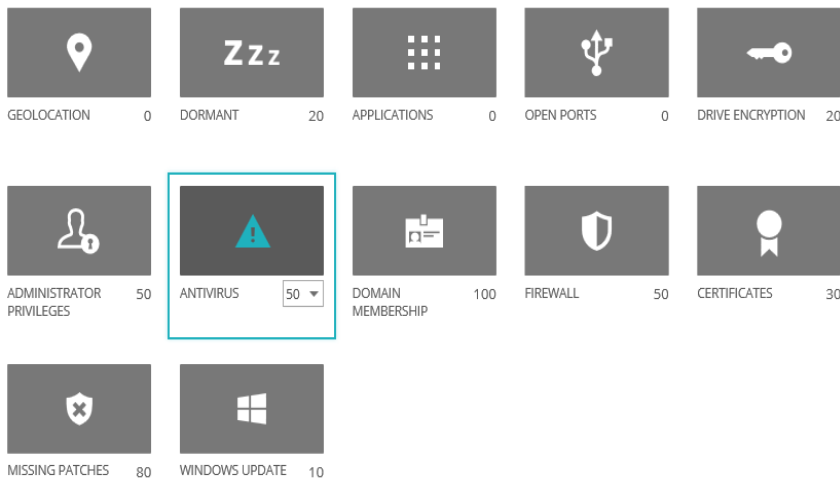
ACCESS CONTROL

- Automated action/access control based on current device risk posture

- Access control across wireless, wired and VPN

- Option to enable two-factor authentication for VPN connections

- Easily set action: allow, alert or block

- Easily customize your risk policy based on access method (wired, VPN, SSID)

GEOLOCATION 0	DORMANT 20	APPLICATIONS 0	OPEN PORTS 0	DRIVE ENCRYPTION 20
ADMINISTRATOR PRIVILEGES 50	ANTIVIRUS 50 ▾	DOMAIN MEMBERSHIP 100	FIREWALL 50	CERTIFICATES 30
MISSING PATCHES 80	WINDOWS UPDATE 10			

TRANSLATING RISK SCORE INTO ACTIONS

■ Allow (0-69)   ■ Alert (70-89)   ■ Block (90-100)

0   70   90   100

Support for IoT and other non-agent devices

Not all devices that need access to the network are able or capable of supporting and agent or supplicant. From the growing Internet-of-Things (printers, VoIP, cameras, etc.) to third party consultants and contractors, you need a solution with the flexibility to safely onboard allowable devices of all types.

Portnox CLEAR provides the flexibility needed to support agentless onboarding of user and non-user devices. Depending on your needs available non-agent access control options include:

○ Active Directory or Open LDAP

○ Portnox CLEAR account via corporate email

○ Portnox CLEAR contractor account via non-corporate email

○ Self onboarding via URL/registration

○ MAC based account (for IoT)

Though you cannot have the device specific awareness and risk-based access controls you gain with AgentP, Portnox CLEAR supports policy flexibility and Dynamic VLANs so you can have control over which types of users and devices are able to connect to which networks and what VLANs.

Groups and Dynamic VLAN

With Portnox CLEAR, you gain the flexibility to define what is allowed where by simply adding accounts (users/devices) into a specified group. Group level policies include:

○ Defined members (users/devices)

○ Available networks (wired, wireless, VPN)

○ Associated risk policy (for AgentP devices)

For example, you could easily create group called VoIP_Phones that includes all company VoIP phones allowing access via your wired network with dynamic VLAN assignment to your voice VLAN.

Cloud Based Wireless & Radius Management

For most SMB's the fear of NAC is not based on lack of ability or appreciation for the awareness, control and security values. It is based on the simple fact that the functions of network administration, network security, and overall IT help desk are often rolled up into one or at most just a few hardworking, always busy individuals — the're the one's working on little sleep with an "S" printed on their chest. We suspect if your reading this, you are very close to one. Good news! Portnox CLEAR is not going to add work, it will actually help reduce some of the most frustrating calls, like the ever popular, "hey what was the wireless password changed too?".

Cloud-based wireless management is one of the hidden values you get with deploying Portnox CLEAR. Simply set-up the wireless SSID(s), authentication type and shared key one-time and that's it. The required client-side information is automatically uploaded to AgentP, so the end user/device does not have to know anything about the wireless access points they have

Add Wi-Fi network

SSID

Authentication type

WEP

Shared Key

access. Should you make any changes, no problem, automatically updated to the impacted user devices. Never again will you have to answer the call, "hey I forgot the wireless password!"

Deploying a traditional on-premise 802.1X based NAC solution brings along with it another management concern in the form of a Radius Server, well really two since you will want those to be redundant. It not so much the additional server resource as it is the configuration and management of Radius — let's face it, Radius is not something even the most seasoned administrator deals with often, so get ready to dust off some old books and manuals. Radius configuration is not walk in the park, configuring authentication with AD, several AD(s), LDAP and allowed protocols on the client/NAS side. And since it really is not something most deal with every day, make sure to leave lots of time for debugging — with many moving parts, just finding where the issue resides can take many hours.

Not to worry, Portnox CLEAR eliminates all the on-premise complexity of Radius by delivering Radius in the cloud. Portnox CLEAR RADIUS service provides a cloud-based cluster of fully redundant Radius servers, can be used for authentication of users accessing the enterprise from wired, wireless or VPN channels. CLEAR automatically generates Radius services for your organization and provides the Radius information you need to configure in your network equipment. Simple, easy, complexity gone!

MANAGEMENT SAVINGS

- Eliminate wireless management of keys, passwords, etc. for end devices
- Wireless changes automatically pushed to affected devices
- No need to configure or manage Radius on premise
- Redundant Radius server in the cloud
- Set it and forget it management.
- Lacks advanced client compliance validation

☑ Enable Cloud RADIUS
Edit

Cloud RADIUS IP:	xx.xxx.x.xxx
Authentication port:	10000
Accounting port:	10001
Shared Secret:	****** Show
Shared Secret expiration:	3:27 PM, 12/25/2016

Guest Management

Portnox CLEAR offers easy and flexible Guest Management! With CLEAR, you simply enable guest management, determine how you want to authenticate guest devices and you are done. With CLEAR guest management you can manage guest in one of three ways:

Disclaimer Only: Devices connecting to the guest SSID will be provided your custom disclaimer/use policy page and once accepted, guest access is granted.

Sponsored Guest: Guests are required to enter a sponsor email. The guest will receive access credentials if the sponsor approves.

CLEAR Guest: The CLEAR administrator must define authorized guests under the CLEAR portal's guest page and send credentials.

Who doesn't like guests (at least for a time)? Portnox CLEAR delivers the flexibility to manage guest in a method that best meets your internal requirements.

GUEST MANAGEMENT

○ Flexible to meet company specific guest management requirements

○ Disclaimer options

○ Sponsored Guest options

○ CLEAR/pre-registered guest options

☑ Enable CLEAR Captive Portal

Url: https://guests.portnox.com/648ab427-c00f-4d88-9c23-828164541379

IP (for walled garden):   104.40.139.161

Authentication type: ○ CLEAR guest
                              ☑ No authentication (disclaimer only)
                              ○ Sponsored guest

Session Expiration: [24   ▼] hours

                              ☐ Ask user to provide email address

Disclaimer ("Acceptable Use" statement):

| Formats ▾ | **B** | *I* | ≡ | ≡ | ≡ | ☰ | ☷ | ⇤ | ⇥ |

This Acceptable Use Policy (AUP) is designed to protect "Portnox", our employees, customers and other partners from harm caused by the misuse of our IT systems and our data.

Misuse includes both deliberate and inadvertent actions.

Logo: portnox™ CLEAR   🗑

[Cancel]   [Save]

Portnox CLEAR Is Different

Organizations of all sizes need real-time clear visibility and control of all devices connecting to their network. The only question is how best to accomplish this goal. For many, cloud services can provide a cost effective manageable alternative to often resource heavy and expensive on-premise solutions. For Network Access Control (NAC), there were no true "born in the cloud" solutions that is until Portnox CLEAR. Portnox CLEAR was designed from the start to be delivered as an easy to deploy, easy to manage, affordable NAC cloud service.

Still not sure? No problem, take Portnox CLEAR for a spin, just visit the website below and start your not cost and no risk trail of our service. Please give us a call or drop us an email if you have any questions.

https://clear.protnox.com/signup