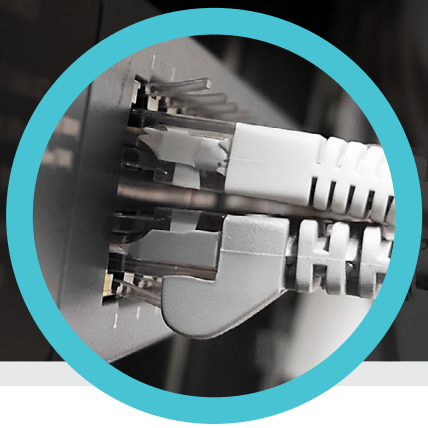
portnox™

Solution Overview

Portnox CORE

On-Premise



Technology Introduction

Portnox CORE provides a complete solution for Network Access Control (NAC) across wired, wireless, and virtual networks for enterprise managed, mobile and Internet of Things devices.

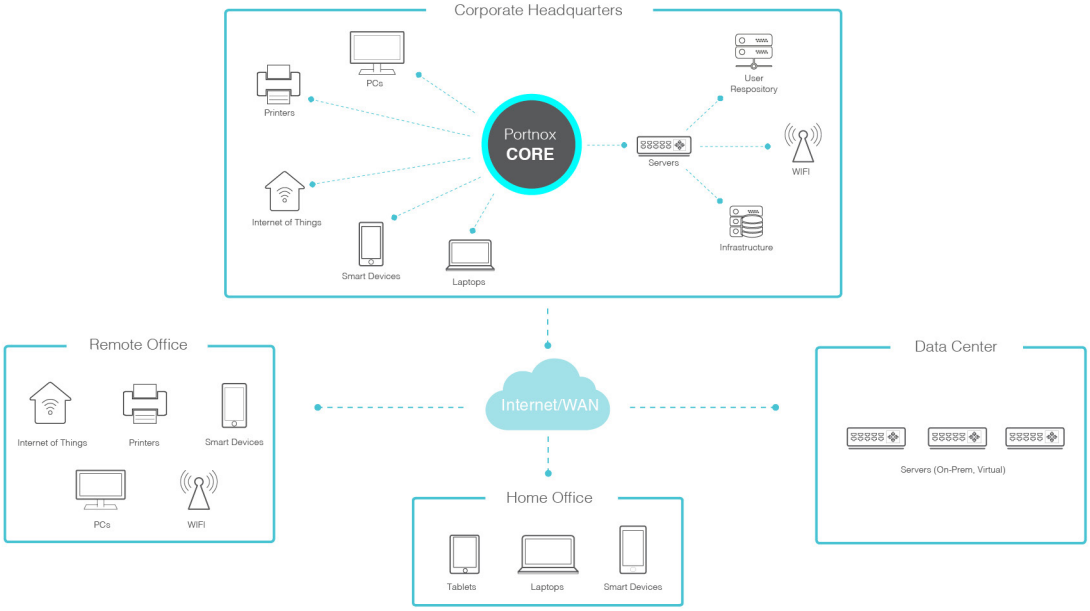
Portnox CORE does not require appliances, agent software, 802.1X or changes to existing networking infrastructure such as mirror or span ports. It supports all existing networking infrastructure and is uniquely adept at handling a wide variety of devices with varying levels of IP support.

Portnox CORE is a software-based solution that runs on Windows Servers (physical and virtual) to continually communicate with all existing networking infrastructure, gaining complete visibility into all assets currently connected to the network. This is achieved through a variety of native connectivity options including SNMP, telnet, SSH, etc. With a definitive and highly accurate view of the network, Portnox CORE can interrogate every connected device to verify its type, patching status, level of compliance, identity and user identity, among other parameters. This is achieved without use of agent software - instead leveraging over 25 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 CORE correlates all knowledge of the device, user, authentication, compliance and location with defined policies to allow access or to take a specific action.

AT A GLANCE

- Centrally Managed
- No Agents
- No Infrastructure Changes
- IoT Visibility Radar
- No Reliance on 802.1X
- Covers ALL Network Layers
- Covers ALL Devices
- Real-Time/Event Driven
- Scalable
- Easy to Manage
- Flexible & Deployable

Portnox CORE Architecture: Network Visibility and Control Across the Enterprise



Portnox Architecture Diagram

As opposed to NAC solutions that rely on port mirroring, IP range scans, inventory directories or other passive methods to obtain device visibility, Portnox CORE directly connects to the network infrastructure via native protocols to provide real-time and immediate awareness of network changes. For example, for managed switches, Portnox CORE can connect via SNMP (read & traps), assuring that Portnox CORE is immediately aware of changes made at the switch level. When a new device connects to a port, Portnox CORE is made aware, often before it learns of the device's IP!

Portnox CORE 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 CORE attempts to authenticate the device (see Authentication) to confirm it is a valid corporate device or designate the device as rogue (see Enforcement).

With Portnox CORE, devices can't hide — if a device is connected to the network and has power, Portnox CORE can see it and control it. Portnox CORE even raises awareness of devices connected to the network via switches not directly managed by the solution.

As a software-based solution, Portnox CORE deploys from a central location, providing network access control across the enterprise – even for remote locations. For environments that require a distributed deployment, Portnox CORE supports this option at no additional cost.

ARCHITECTURE HIGHLIGHTS

- Natively connects to network infrastructure elements
- No agents to deploy
- No reliance on 802.1X
- Real-time, event driven device awareness
- Software-based, no appliances
- Central or distributed deployment based on network at no additional cost

Real-Time, Continuous Device Discovery

As outlined above, Portnox CORE starts at the infrastructure layer. Connecting directly to wired, wireless and virtual infrastructure, Portnox CORE delivers real-time, continuous and event-driven visibility into and control over all devices connecting to the network.

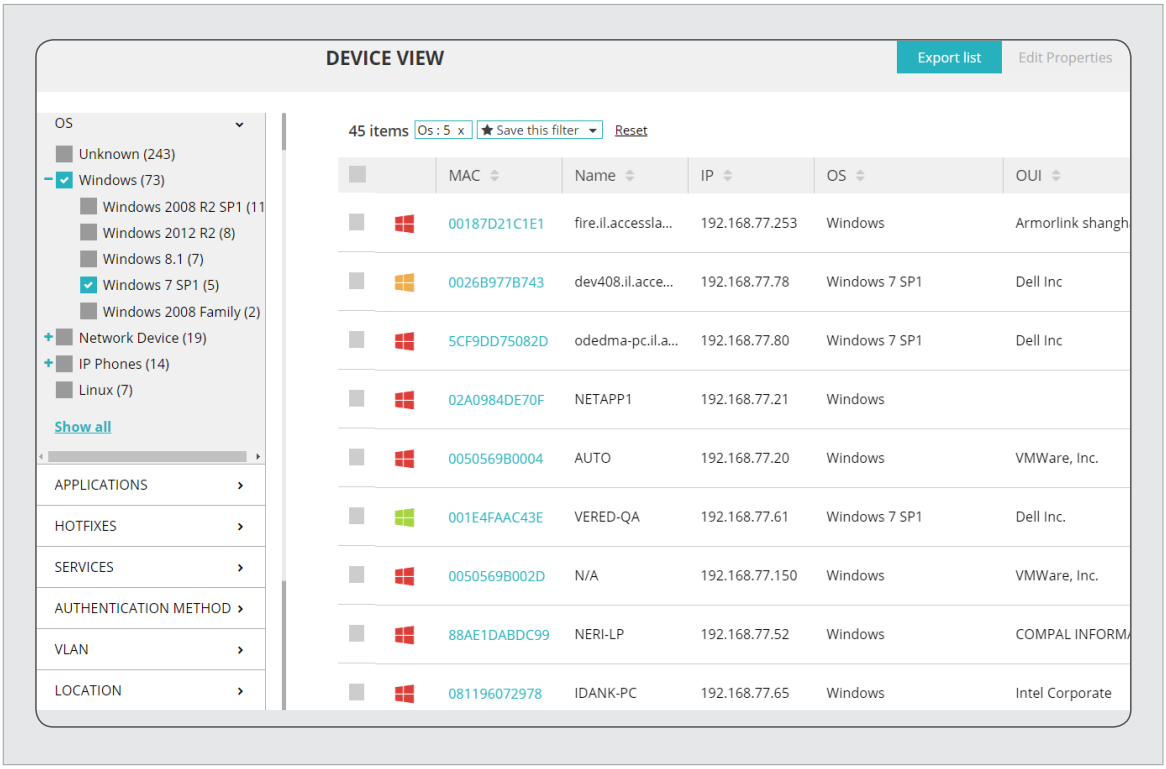
Portnox CORE's configuration options support continuous validation of devices previously onboarded to ensure they maintain compliance while connected to the network. If there is a converged VoIP environment Portnox CORE can automatically detect, discover and validate VoIP phones and connected devices.

Portnox CORE discovers, notifies and can takes actions against unauthorized hubs or access points. If authorized, Portnox CORE provides discovery, authentication, and control for each device independently.

Portnox CORE provides both a Network View and Device View with easy search options to quickly locate any device, user, IP/MAC, application and more. Beyond NAC, Portnox CORE's Network/Device view and its extensive search capability provides an answer to daily operational and help desk tasks by quickly answering the question "Where is xxx on my network?".

NOTHING CAN HIDE

- Discovery starts at the infrastructure layer
- Real-time/Event driven
- Continuous and on-going
- No passive IP range scans, port mirroring
- Easily create device filtered views based on device attributes including: OS, active applications, location, security status and more



Internet of Things (IoT) Visibility Radar

Internet of Things (IoT) devices are being adopted by enterprise on a massive scale due to their benefits in increasing productivity and advanced data mining capabilities. However, many of these devices do not come with built-in security settings or patching options, leaving the network open and exposed to vulnerabilities.

Portnox CORE, through its IoT Visibility Radar, offers a complete visibility solution for discovering IoT devices that includes detailed information about the endpoints, such as OS, open ports, and running services, as well as alerts for changes in their behavior on the network. The IoT Visibility Radar detects these changes by employing dual fingerprinting: Portnox CORE's proprietary solution for automatic device discovery (OSFP) together with SNMP/NMAP tools. This allows security auditors and network admins to verify and track changes in the connectivity of IoT devices on the network, raising awareness of potentially suspicious behavior and vulnerabilities. The IoT Visibility Radar completes the detection and discovery of IoT devices and changes in their status within minutes, allowing admins to make rapid and informed decisions regarding the state of their network.

For example, if an IoT device is compromised, it will be detected by the IoT Visibility Radar as a possible rogue device if a new service, such as FTP, has been opened on the device. Portnox CORE will issue an alert if a policy action is configured to respond to the event and automatically perform remediation measures, such as blocking or quarantining the device.

Device Authentication

Once discovered, the next step is authentication. As with infrastructure connectivity, Portnox CORE authenticates corporate devices natively without the need for an agent, supplicant or "dissolvable" agents. Portnox CORE 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 BYOD and Internet of Things (IoT) devices.

Portnox CORE goes the extra mile, for example in a VoIP environment, by not only providing strong authentication (typically via SNMP or OSFP), but also through integration with an on-premise VoIP PBX to obtain additional details on the VoIP device including extension number. This information then becomes available and searchable. Want to know where VoIP extension 5066 is connected? With Portnox CORE, it's a click away!

AUTHENTICATION VALUES

- 25+ Authentication Methods
- No Agent
- No Supplicants
- No "Dissolvable" Agent
- Strong, Secure Authentication for IoT devices
- Voucher for time-limited device authentication

Enforcement & Compliance

There are numerous solutions and methods for discovering devices connected to the network, but the real value of NAC is being able to proactively take enforcement actions on devices that do not belong on the network or are not within security/compliance risk tolerance. However, most traditional NAC solutions do not have the level of device awareness or enforcement flexibility required for companies looking to move to full enforcement, resulting in the use of NAC as simply a device discovery solution.

That is not the case with Portnox CORE. Most of our customers deploy with full enforcement enabled. Why? Because the solution is simple, provides device awareness, actionable intelligence and enforcement flexibility!

We have already covered how Portnox CORE works from the infrastructure layer up and that the solution optimizes the network management experience by integrating with PBX, AD and other device knowledge bases to gather as much detail on connected devices as possible.

We have yet to mention that Portnox CORE also connects back to corporate endpoints without an agent to perform compliance and validate the device against a wide variety of checks including: OS, AV, active NIC(s), local user privileges, removable storage, authorized (or unauthorized) programs, services and more. And if an endpoint management solution is already in place, Portnox CORE can check it's view on device status as part of compliance validations.

Yet what truly separates Portnox CORE from other NAC offerings is the flexibility it offers in taking enforcement actions based on the device, user, authentication, location and level of compliance. Flexibility is critical for companies that want to achieve a healthy balance between security and productivity.

Portnox CORE's flexibility extends to device onboarding, support for pre-connect/post-connect and a hybrid partial pre-connect onboarding model. There is even the possibility of selecting different on-boarding methods for different network segments, VLANs or groups.

Finally, Portnox CORE's flexibility extends from roll-out and migration; from discovery to enforcement — start in monitor/discovery mode and slowly roll-out automated enforcement to specific ports, switches, VLANs or locations. With Portnox CORE, deployment is a walk in the park!

ENFORCEMENT

- Flexible enforcement actions based on device, user, location, authentication, compliance
- Detailed endpoint compliance checks and validation
- Easily phase in enforcement to assure success
- Seamlessly balances between security and productivity

Secure Enterprise Mobility – Portnox CORE & CLEAR

Portnox offers a unique hybrid solution that pairs the strength of on-premise NAC offered by Portnox CORE, with the cloud secure risk-based access of Portnox CLEAR. Portnox CORE can be configured to work hand-in-hand with Portnox CLEAR to provide a solution that addresses some of the major challenges of enterprise mobility, such as:

- **BYOD:** Gain visibility and control over both managed and unmanaged devices, mobile, tablet, desktop and "smart" gadgets, that connect over the enterprise network. Building on Portnox CLEAR's strengths as an "always-on" cloud solution, integration between Portnox CORE and CLEAR is an important security solution for enterprises that encourage their employees to work off campus, but want to remain in control of what they can access when. By assessing each device's unique risk-score, Portnox CLEAR takes the organizational security policy into account, factoring in a device's specific level of risk and vulnerability.
- **Secure Guest Management:** Portnox CLEAR enables flexible guest management for the enterprise that wants to encourage work with external players, but wants to ensure that their network is secure and unauthorized access is prevented. In the Portnox CORE and CLEAR integration, some of the guest management features that are offered include: disclaimer-based access, sponsored guest access, or multi-factor verification at access. Whatever the guest access needs of the organization, Portnox can meet them.
- **VPN Controls:** More employees working remotely creates a need for stronger controls on VPN access. With a Portnox CORE-CLEAR support for, gain the strength of on-premise-level security for remote VPN access. With continuous and real-time device risk posture assessments, set specific security controls for VPN access that addresses device-level risk. Portnox CLEAR also offers an option for multi-factor authentication when accessing VPN networks, and options to set group and dynamic VLAN policies specifically for VPN access.

For more information on our secure enterprise mobility solution –

CONTACT US

Get to the CORE of Your Network

Organizations of all sizes should have real-time visibility into and control over all of the devices connecting to their network. The only question is how best to accomplish this goal.

At Portnox, we focus on only one thing — that is, how to deliver network access control solutions that provide 100% visibility and control of all devices on the network (wired, wireless, virtual). Our solutions are designed with ease-of-use, ease of deployment and flexibility in mind, making them scalable across enterprises of all sizes.

That said, words are easy to write — our preference is that you see how Portnox CORE works!

Request a Demo Now

Or Contact Us!

Contact Us

Americas: usinfo@portnox.com | +1.855.476.7866
Europe: dotell@portnox.com | +44.1273.256325

www.portnox.com

www.twitter.com/portnox
www.facebook.com/portnox
www.linkedin.com/company/2526271/
www.youtube.com/portnox

portnox™